Exhibit 2.3.1 – MODIFICIATION NO. 9
Solution – End User Devices and Hardware

Effective 11/29/2021

VA-180915-IBTL: End User Services-Computing

COMMONWEALTH OF VIRGINIA
VIRGINIA IT AGENCY (VITA)
SUPPLIER STRATEGY AND PERFORMANCE DIVISION
11751 MEADOWVILLE LANE
CHESTER, VIRGINIA 23836

Table of Contents

1.0 Introduction

For successful delivery of the End User Services – Computing (EUC) Devices and Hardware, Iron Bow will use an approach that has Information Technology Infrastructure Library (ITIL) methodology at its foundation. The ITIL framework is renowned for its holistic approach to Information Technology (IT) service delivery; it provides a framework for the governance of IT and the management and control of IT services. ITIL provides Iron Bow with a focus on the continual measurement and improvement of the quality of IT services delivered from both a business and a customer perspective. This focus will be a critical factor in Iron Bow's successful deivery of the solution by helping to consistently deploy standardized techniques and processes throughout the Virginia Information Technology Agencies (VITA) Environment in conformance with the Service Management Manual (SMM). Iron Bow will use ITIL to establish a baseline to plan, implement and measure EUC support services during integration with the Multisourcing Service Integrator (MSI) and Service Tower Suppliers (STS).

2.0 Common Services

Iron Bow understands that there is a variety of common services to be performed. Table 1 below indicates Iron Bow's acceptance of those requirements.

Table 1 Common Service Requirements

Common Service Requirements
Iron Bow will: • Adhere to and perform the Cross Functional requirements contained in Exhibit 2.2 (Description of Services - Cross Functional) • Integrate Iron Bow's Service Management components with the MSI's Service Management System (SMS) through industry standard interfaces for bidirectional communications between the STS tools and SMS • Work with the MSI to ensure that the SMS remains the central and common database and path to process participation, ensuring operational oversight and compliance • Provide VITA and Customers a multi-tier Support Level Environment (e.g. variety of standard offerings in "tiers" or "bundles", optional enhancements, etc.) • Deliver customer-focused services that are responsive to their needs, resolving issues rapidly and at the lowest level of support • Provide EUC onsite support as required in the support level (e.g. VIP, gold, silver, bronze) • Provide white-glove VIP User support on a 24x7x365 basis • Work cooperatively with STS's in delivering Smart Hands support • Provide ability to reduce or enhance support on a temporary basis, up to and including 24x7x365, as an optional service (which may be a short-term or long-term basis to support cyclical business needs, seasonal surge, administration changes or emergencies, etc.) by Site or Customer • Implement services to ensure confidentiality, integrity, privacy, and authenticity of the information stored in and/or transmitted to/from the Managed Environment, in accordance with the VITA Rules • Work collaboratively with VITA, MSI, other STS's to foster an environment of continuous process improvement; participate in MSI quality assurance and continuous process improvement meetings and initiatives

- Drive continual service improvement of provisioning processes to ensure processes are up to date and do not conflict with any new or upcoming changes that may impact the enterprise and complies with VITA Rules

2.1 General

1. Provide effective end-to-end management, monitoring, and reporting in accordance with the SMM and VITA Rules

The solution Iron Bow has designed and will deliver to VITA to provide EUC incorporates Cherwell Service Management, Cherwell Asset Management, Microsoft Deployment Toolkit (MDT), Microsoft Service Center Configuration Manager (SCCM), [redacted]. Iron Bow will integrate Cherwell, SCCM, and [redacted] to provide automated functionality, and will integrate the Iron Bow tools with the MSI SMS to provide end-to-end management, monitoring and reporting to the Devices covered under the consumption model.

Iron Bow will establish alerts within each of these tools to notify the Service Operations Manager when service levels and key measurements fall outside of the defined requirements. The following describes events once an alert is triggered:

a. Pre-set alerts notify Iron Bow of the issue prior to Customer noticing an issue
b. Field Service Technician assigns an internal ticket through the SMS
c. Field Service Technician investigates issue and proactively applies fix, including researching the known error database or developing a work around
d. If Field Service Technician is unable to fix the issue, he or she creates a Problem ticket that initiates Problem Management process
e. Field Service Technician and Subject Matter Experts perform root cause analysis
f. Root cause identified, corrective action taken, entries added to the known error database, and changes made in accordance with Change Management procedures
g. For any reporting requirements, Iron Bow will use the integration of Iron Bow's tools with the MSI's, to customize reporting and dashboards to provide real time information to VITA, the MSI or other STS's

Iron Bow has selected and will provide tools to meet VITA's EUC needs based on: 1) size of the Enterprise; 2) variety of business needs and size of Customers; 3) types and mix of Hardware, Operating Systems and applications; 4) scalability and flexibility; and 5) ability to integrate with other tools.

Additionally, the tools Iron Bow has selected and will provide, will be used within EUC to support internal operations and integrated with the MSI's toolset using industry standard interfaces to allow for real-time, bi-directional communication. Iron Bow will collaborate with the MSI to ensure that the SMS remains the single source of information for VITA and Customers. Iron Bow will collaborate with the MSI to design the appropriate interfaces to ensure real time information flow.

Should any integration between Iron Bow's proposed tools and the MSI SMS fail, Iron Bow will collaborate with the MSI to utilize their tool suite.

2. Provide, maintain, and support procedures for Users that are not connected to the production network every day to ensure Patching levels are current and accounts do not expire in accordance with SMM and VITA Rules.

Iron Bow will use their Microsoft SCCM platform to control, get information from, Patch and apply applications to all EUC Devices. Several key features of SCCM support User centric management, which will address the bring-your-own-Device (BYOD) trend as it becomes more prevalent in the enterprise. Users will have the ability to search for applications with a self-service Software center and specify times when installations and upgrades take place or to download the Patches themselves. Through SCCM, Iron Bow will develop and document a contingency plan that will include descriptions of how applications may be installed in different ways on different Devices; which may include for example, as a native application on a primary Device or as a remote desktop services app or App-V program on a tablet. SCCM also includes and Iron Bow will provide role-based access control (RBAC), which enhances system security by only showing Users the interface elements that apply to their specific role as defined by Active Directory. Iron Bow will also employ [redacted] to maximize the investment in SCCM. [redacted] will be used by Iron Bow to provide increased capability in supporting Patches on Devices that are disconnected from the network.

Iron Bow will utilize the process described below to ensure that off-network and intermittently-connected Devices are Patched and compliant with the procedures specified within the SMM and VITA Rules. Field Service Technicians will support the Hardware and Software Services team in this effort.

Iron Bow, in conjunction with VITA, Customers, the MSI, and MSS, will evaluate each offline Patching requirement to ensure the update frequency/cadence meets the MSS/MSI security standards and the VITA Rules. All Patch levels will be maintained by Iron Bow as per the requirements defined in the SMM, unless noted as an exception and subject to the defined exception processes outlined in the SMM. Additionally, in such cases where a critical Patch/update is required out of schedule, Iron Bow will coordinate with VITA, Customers, the MSI, and MSS to assess overall criticality and potential impact for each offline requirement, determine accessibility to Devices, define a Patching order and/or schedule and address each requirement as agreed and in accordance with the process outlined in the SMM. Iron Bow's process is as follows:

Baseline: Audit all off-line machines and Patch to agreed Patching level baseline; conversely, reimage all offline machines to a common image with known Patching level. This will be a manual process. Once Iron Bow has a solid baseline, the Offline Patch Deployment Process, described below, will be implemented by Iron Bow.

- Windows Machines
  - Define Patching schedule/frequency to match VITA requirements
  - Leverage WSUS Offline Update (or other tool) to compile and download all appropriate Patches based on defined baseline OS and Office versions.
    - With Windows 10, leverage Monthly Quality Updates to manually update machines to the required Patch level and 2x per year to deploy feature updates manually.
  - Create update media (USB or DVD ISO) containing Update Installer Software and required Patches.
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
  - Analyze log files to ensure completion and no errors are present
  - Create Offline Machine Patching Report Data
- Mac/Linux Machines
  - Define Patching schedule/frequency to match VITA requirements
  - Leverage [redacted] of Linux/Mac to create offline Patching package.
    - [redacted]
  - Execute offline patching package and deploy patches to Mac/Linux machines.

- Analyze log files to ensure completion and no errors are present.
- Create Offline Machine Patching Report Data

Internet Based Patching: Iron Bow will provide and use the [redacted] to deliver updates to internet connected clients. The [redacted] provides management of internet-based clients. It uses a combination of a Microsoft Azure cloud service, and a new site system role that communicates with that service. Internet-based clients use the cloud service to communicate with the on-premises Configuration Manager. Deployment and operation of the [redacted] includes the following components:

- The [redacted] in Azure authenticates and forwards [redacted] client requests to the [redacted] connection point.
- The [redacted] connection point site system role enables a consistent and high-performance connection from the on-premises network to the [redacted] in Azure. It also publishes settings to the [redacted] including connection information and security settings. The [redacted] connection point forwards client requests from the [redacted] to on-premises roles according to URL mappings.
- The service connection point site system role, runs the cloud service manager component, which handles all [redacted] deployment tasks. Additionally, it monitors and reports service health and logging information from Azure Active Directory (AD) to ensure your service connection point is in online mode.
- The management point site system role services client requests per normal.
- The software update point site system role services client requests per normal.
- Internet-based clients connect to the [redacted] to access on-premises Configuration Manager components.
- The [redacted] uses a certificate-based HTTPS web service to help secure network communication with clients.
- Internet-based clients use [redacted] for identity and authentication.
- A cloud distribution point provides content to internet-based clients, as needed.

Iron Bow will provide the follow:

- An Azure subscription to host the [redacted]
  - An Azure administrator needs to participate in the initial creation of certain components, depending upon your design. This person does not require permissions in [redacted]
- At least one on-premises Windows server to host the [redacted] connection point.
- The service connection point in online mode
- A server authentication certificate for the [redacted]
- Azure Resource Manager deployment model
- Other certificates may be required, depending upon the Customer's OS version and authentication model
  - Configure all [redacted] enabled management points to use HTTPS
- Integration with Azure AD for Windows 10 clients
- IPv4

All EUC Devices, excluding those that are in offline service status, are required to report every 14 days. When a Device has not reported in 14 days and their CI does not have a designation stating it may never report, Iron Bow will configure Cherwell to issue an automated ticket to investigate the status of the Device. Once the status of the Device is determined, the CI will be revised to reflect the appropriate designation as defined in the SMM.

3. Support the MSI and respond as required to de-provisioning requests (including handling investigations and terminations on an emergency basis) in accordance with the SMM and VITA Rules.

Iron Bow Field Service Technicians will support de-provisioning requests upon receipt of a Service Request as submitted through the MSI SMS. Iron Bow will integrate the enterprise Cherwell Service Management with the

MSI's SMS to ensure information is bi-directionally shared between both systems in real-time. The codeless Environment of Cherwell and ease of implementation will provide additional flexibility as Iron Bow evolves Services. To exchange information with the MSI, Iron Bow will build an interface to allow the MSI to push tickets seamlessly, as well as enable ticket replication in the MSI tools for those created in Cherwell, as required. Cherwell will also be used for Asset Management, Knowledge Management, and the On-line Application Store in concert with Iron Bow's other tools, such as Microsoft SCCM. While other tools may be used within EUC, Iron Bow understands that the single point of truth will remain with the MSI's SMS. Iron Bow and Cherwell will work during Implementation to ensure the proper interfaces are designed and working as intended for bidirectional, one directional, real-time, or batch uploads – as determined appropriate/required by VITA.

4. Communicate to Users in English, using terms that are clearly understood by the Users and consistent with those used by Customers.

Iron Bow EUC personnel will be required to communicate in English, using terms and provide guidance that is clearly understood by the general population of Users. Iron Bow will seek assistance through training materials, knowledge management articles, and other learning aids to supplement support.

5. Identify, build, and conduct User training in accordance with VITA Rules and the SMM.

Within the offered Services, Iron Bow will support User training at no additional cost. Iron Bow will provide the resources needed to identify, build and conduct User training.

In order to address VITA User training needs, Iron Bow will conduct a training needs analysis to identify problems or other issues in the workplace to determine whether directed training is needed. During the needs analysis, Iron Bow will collect and document information concerning performance problems or the anticipated introduction of new systems/applications, tasks or technologies. Iron Bow's needs analysis will save time and effort by defining training to address the most common problems. There are a number of practical methods Iron Bow will use to gather this data such as interviews with VITA or VITA Customers, brief questionnaires, and ticket trends. After Iron Bow assesses the training needs and levels, the information will be provided to VITA for review and approval in accordance with the processes described in the SMM.

Iron Bow will support the MSI in the development of training materials. Materials needed to conduct the training such as presentations, brochures, "How-To" or quick help guides, tip sheets and manuals are created, updated and maintained by Iron Bow in the MSI's Document Library. Training will be requested by the Customer through issuance of a Service Request to the MSI within the SMS. The MSI will issue a Service Request to Iron Bow to request training support. As Iron Bow supports the development of training materials, any multimedia visual aids and presentations will be Section 508 compliant. The Service Request from the MSI should include, but may not limited to: supporting training instruction, providing training on individual products or Services, or training as part of an implementation project of a new technology or Service.

6. Provide recommendations on Knowledge Base entries in accordance with the SMM and VITA Rules.

Iron Bow will utilize Cherwell (as integrated with the Service Knowledge Management System (SKMS) provided by the MSI) to capture, store, and present information needed to manage and consume the Services. Iron Bow staff supporting resolution of requests will use the information stored in the SKMS to be more efficient in solving/completing requests. Iron Bow will not only contribute to producing knowledge articles, scripts, How To Guides and Frequently Asked Questions but will also create and maintain self help articles, which include but are not limited to: knowledge articles, how to guides and frequently asked questions. Iron Bow's Quality Assurance Team will conduct, no less than annually, a review of knowledge articles to determine which ones remain current and apply to existing Services and where new articles are needed. The Quality Assurance Team will provide the feedback to the MSI and make the changes in accordance with the process in the SMM.

7. Perform and document systems tests and implementation plans on all Hardware/Software created, owned, deployed, or managed by the Supplier.

Iron Bow will perform system testing of Hardware/Software to evaluate compliance with its specified requirements. Iron Bow's EUC Functional Area Teams (PC Refresh, Imaging and Patch) will prepare test plans that establish the scope, approach, resources and schedule of intended test activities. All tests will be performed in Iron Bow's dedicated test lab. For the test results to be useful, Iron Bow will ensure that the lab Environment reflects the production Environment as closely as possible. The test lab will be updated as the production Environment changes to ensure Iron Bow's results resemble performance in the User Environment. Test results will be documented and provided to VITA as required. Testing will include the following: Customer completion of functional testing; systems integration testing; data conversion procedures; LAN/WAN connectivity testing; system load, reliability and performance testing; regression testing; application inter-connectivity testing which simulates Customer's production Environment – including with commercial off the shelf (COTS) and custom-developed applications for compatibility; user acceptance testing (UAT) of a complete application; and Customer approval to release to production. Testing activities will be coordinated with and reported to the MSI in accordance with the SMM.

8. Provide the ability to send targeted communications directly (i.e., non-e-mail) to individual workstations, Users, Customers, or Sites, issuing instructions or specific requirements (e.g., during a Security or disaster event, to provide instructions on Patches or inventory, etc.) in accordance with the SMM and VITA Rules.

Iron Bow will use SCCM to send targeted communications directly (i.e., non-e-mail) to individual workstations, Users, Customers, or Sites, issuing instructions or specific requirements (e.g., during a Security or disaster event, to provide instructions on Patches or inventory, etc.) in accordance with the SMM and VITA Rules.

There may be time for important services to be brought offline temporarily, for scheduled maintenance or for upgrades and impact to Users is unavoidable. Iron Bow will coordinate with the MSI for any messaging to End User regarding Software distribution/Patching. In coordination with the MSI and to the extent possible, Iron Bow will give Users, at a minimum, 5 days' notice for planned downtime. This will give Customers enough time to prepare themselves and to mitigate the effect on their work Environment. The larger the impact on Users, the longer the lead time needs to be. Depending on the expected impact, Iron Bow will send multiple notices. Not all Users will remember a single notice, so Iron Bow will use multiple notices to keep reminding them as the scheduled time gets closer. If possible, Iron Bow will communicate the upcoming downtime using multiple channels. Iron Bow will communicate via web pages, internal communication methods (e.g. the Imaging Team) or on the application's start page, as appropriate. The best medium will depend on the User base and the timing of the update. For applications, Iron Bow will place a notice about upcoming downtime on the login page or main start page as far in advance as possible, so that Users are able to plan their work around the downtime. If the affected application is a smartphone app, Iron Bow will add in-app notifications or push notifications. Iron Bow will also follow up after the systems are back online to let Users know that the downtime is over and systems are once again available.

9. Maintain ongoing institutional knowledge of VITA and Customer Environment via knowledge capture processes and personnel retention policies.

Iron Bow will overcome the rapidly accelerating loss of institutional knowledge by building an explicit strategy for maintaining institutional memory and ensure the knowledge base remains solid. The knowledge capture strategy includes: collecting knowledge from the Field Services Technicians, revising or establishing new policies or procedures incorporating that knowledge, collect knowledge through knowledge articles in the Knowledge Management System, share knowledge, and develop and conduct training to ensure knowledge is shared. A summary of Iron Bow's process is as follows:

1) Gather:
    a. The Transition Manager and Team will gather information during the skills and operational assessment of the Field Services Technicians discussed in Section 2.2.
    b. Document all existing processes and workflows
    c. Document ticket resolution as knowledge articles and provide them to the MSI to be stored in their Document Library
2) Analyze the data: From the data gathered, Iron Bow's Transition Manager and Program Director will identify the key data points that Iron Bow wants every member of the End User Computing (EUC) staff to know or be able to do and turn this from an implicit assumption to an explicit expectation. This knowledge will be documented in policies and procedures and published in the MSI Document Library
3) Develop training: Iron Bow will develop and conduct training around EUC area of responsibility topics so that the knowledge is shared. Iron Bow will also use this information at orientation sessions for new personnel.
4) Store the knowledge: Iron Bow will use technology (e.g., the Knowledge Management System within Cherwell (as integrated with the SMS) to create a process by which EUC staff continually captures and correlates institutional knowledge. Iron Bow will use this as a living and evolving body of useful information that is accessible to people as they join the organization.
5) Continuous process for evolving knowledge: Through the resources within Iron Bow's Training and Quality Assurance Teams, Iron Bow will continually assess performance of individual Field Services Technicians, overall performance metrics/SLAs, customer satisfaction, and any customizations/changes to the Environment to ensure Iron Bow is maintaining the appropriate skills and abilities.

Iron Bow will also build and provide information to the MSI for electronic "Site Books" for each Agency. Our team will provide knowledge about each Agency relative to site access, Agency-specific applications or Software, specialized equipment needs, support hours, and VIP level support at the Agency which will be used to develop the site books. These books will also include maps of the facility, telecommunication closet locations, and wiring diagrams. Iron Bow's Transition Team will start working on collecting this knowledge upon Effective Date. This information will be used as reference material in the event there are coverage changes and for orientation of new staff to lessen the learning curve.

From a personnel perspective, it is Iron Bow's objective to re-badge those incumbents who are performing successfully. Iron Bow will use a variety of methods to attract and capture the incumbents. Incentives include sign on bonuses, comprehensive compensation plans, competitive benefits, 401K packages, and employee perks (e.g., continuing education, certification training, and employee discounts). Iron Bow's ability to retain quality technical personnel is the result of its management philosophy and environment – which defines Iron Bow's culture. Iron Bow takes pride in being a "people-oriented" company, respecting each employee and his or her rights as a worker, and furnishing a working environment conducive to professional challenge and advancement opportunity. Iron Bow's wage and salary structures are geared to fairness and equity, and Iron Bow's employee benefit plans are reviewed and updated regularly. All of these features lead to high morale, excellent employer-employee relations, and a motivated team that provides outstanding performance.

Iron Bow will provide a built in career ladder progression for staff assigned to this contract. Iron Bow will promote from within at all levels, beginning with PC Refresh. PC Refresh is an entry level position through which an employee could gain additional skills to move into a Field Service Technician (which has multiple levels of progression). From Field Services Technician, an employee has the ability to move in a number of different capacities such as Quality Assurance, Training, Imaging, Patching, or Project Team Leadership. Career

progression provides opportunity to increase skills and pay, therefore maintaining talent and knowledge on the Program.

10. Evaluate and test all applicable Patches, releases, service packs, upgrades, and configuration changes in a test Environment, to include regression testing in accordance with the SMM and VITA Rules.

The breadth and detail of Iron Bow's solution for Patch, release, service packs, upgrades, and configuration changes will relate directly to the criticality of systems and data handled and the complexity of the Environment (e.g. number of supported platforms and applications, number of remote offices). Iron Bow's testing process will begin with acquiring the Software updates/release/service pack and continue through acceptance testing after production deployment. The first component of testing will be the verification of the source and integrity of the Patch/release/service pack/upgrades/configuration change. By including this step in the process, Iron Bow's Hardware and Software Services Team will ensure that the update is valid and has not been maliciously or accidentally altered. Digital signatures or a form of checksum or integrity verification will be a component of Patch validation. This signature will be regularly verified, especially as an update is passed through operations (e.g. on the update server, in build images, in Software repositories).

Once a Patch has been determined valid, Iron Bow will place it in a test Environment. Iron Bow's Hardware and Software Services Team will mirror the production Environment as closely as possible. It is important to at least account for the majority of critical applications and supported operating platforms in the Patch testing infrastructure. There may be instances where a subset of production systems will serve as an ad hoc test Environment; IT employee systems are typically used in these cases. Regardless of the available test equipment and systems, Iron Bow understands it is critical to and will expose the update to as many variations of production-like systems and End Users as possible to ensure a smooth and predictable rollout. In such cases, Iron Bow will submit a request to VITA for approval prior to any changes being made to the production Environment.

The actual mechanics of testing a Patch may vary widely. This testing may be simply installing a Patch and making sure the system reboots or the test procedure may involve the execution of a battery of detailed and elaborate test scripts that validate continued system and application functionality. Iron Bow will use a suitable approach toward detailed Patch testing which will be dictated by system criticality and availability requirements, available resources, and Patch severity.

The initial phases of production rollout will be an additional component of the testing process. In coordination with the MSI, Iron Bow will perform rollouts in tiers. The initial tiers will involve less critical systems. Based on the performance of these stages of the Patch deployment process, the entire Environment will be updated, and the testing process will be considered finished with the successful completion of final acceptance testing.

11. Make all documentation pertaining to tested changes available to VITA authorized or designated personnel (which may include Customer representatives or other suppliers) in accordance with the SMM.

Within Iron Bow's testing process, Iron Bow defines 5 phases that will be documented in a comprehensive Test Plan which includes processes for: test planning; test design; test execution; test validation and release; and test documentation. Iron Bow will perform testing, validation, and release against the plan on Devices, OS, applications, and any changes made thereto. Iron Bow will document all test results using industry best practices and provide the test results upon request and pursuant with the SMM requirements. Documentation will be maintained in accordance with VITA's Change Management procedures.

12. Provide the ability to deliver all the security and audit logs to VITA authorized or designated personnel (which may include Customer representatives or other suppliers) in accordance with the SMM.

Iron Bow will coordinate with the MSS provider to maintain the security and audit logs, as required by VITA and documented in the SMM. An Operating Level Agreement (OLA) will be added between Iron Bow and the MSS regarding access to these tools. These security and audit logs will provide:

- Accountability. Log data identifies what accounts are associated with certain events to highlight where training and/or disciplinary actions are needed.
- Reconstruction. Log data reviewed chronologically to determine what was happening both before and during an event. For this to happen, the accuracy and coordination of system clocks are critical.
- Intrusion Detection. Unusual or unauthorized events detected through the review of log data will include failed login attempts, login attempts outside of designated schedules, locked accounts, port sweeps, network activity levels, memory utilization, and key file/data access.
- Problem Detection. Log data used to identify security events, e.g., investigating causal factors, resource utilization, trending and so on.

13. Maintain spare supported End User Devices to enable Incident Resolution and Device repair, including support of remote sites, within specified SLAs.

The management of spare Devices/parts and other materials needed for realization of the maintenance process is one of the key functions in Iron Bow's approach to physical asset management. Iron Bow will have locations across the Commonwealth where Iron Bow will maintain inventory that is used to do hot swaps.

By maintaining spare parts at Iron Bow's warehouse facilities and other office locations, Iron Bow will:

- Increase service level of inventory: The systems Iron Bow uses, such as Cherwell linked to SCCM, will drive efficiency in the spare parts planning – right parts, right time.
- Improve equipment uptime: Our process for maintaining and deploying spares decreases and increases first-time fix rate.
- Decrease investment in inventory: Iron Bow will use historical data and data from our systems to find the optimal balance between stocking levels for inventory and the investment made into spare parts. An effective spare parts management and planning system reduces inventory while still maintaining high levels of service and accessibility.

14. Act as Subject Matter Experts (SMEs) on all standard Software and Hardware that comprise the User's client.

Iron Bow will re-badge incumbent employees who are performing well supporting VITA. This will ensure that Iron Bow has incumbent knowledge, vendor and infrastructure specifically, to serve as SMEs. Additionally, through Iron Bow's corporate partnerships with Original Equipment Manufacturers (OEMs), Iron Bow is required to maintain levels of corporate, as well as individual certifications. As a result, Iron Bow maintains the highest certifications across all of the top tier OEMs in the VITA infrastructure. These experts are resident within Iron Bow and will serve as SME resources to support Iron Bow on-site personnel. These SME resources include: Solution Architects; Implementation/Deployment Engineers; Consulting System Engineers; System Integration/Sustainment Engineers; and Application Developers/Business Analysts. Our SMEs hold the highest level certifications across Dell, HP, Microsoft, VMware, EMC, and Cisco, and are experts across a variety of areas such as: desktop computing, data center, collaboration/unified communications, security, next generation networking, wireless, audio-video, and mobility. These SME engineers serve as mentors and escalation points for Iron Bow on-site teams. The SMEs are available to Iron Bow's EUC program staff to: troubleshoot complex issues; work with OEMs for technical assistance or warranty support; provide onsite advanced diagnostics; conduct assessments; and deploy tools to provide recommendations on replacements/upgrades of Hardware/Software solutions. These resources are available in person, by phone, or video teleconference to support Iron Bow on-site personnel.

15. Provide additional temporary resources as needed or at VITA's or the MSI's direction in the event of a Major Incident, Problem, or Event to restore Services to the normal state.

The Iron Bow Program Director and Service Operations Manager will jointly oversee the process defined in the SMM for managing Major Incidents, Problems, or Events from identification through closure, as directed by VITA and coordinated with the MSI. In accordance with the MSI's Major Incident, Problem and Event procedures, Iron Bow will assign subject matter experts or other resources as requested to support resolution. SMEs or other resources assigned will treat the resolution of Major Incidents, Problems, and Events as top priority regardless of other work assignments; Team Leads will re-assign staff to cover existing workload while the Major Incident is worked.

Iron Bow will review, diagnose, and resolve the issue as quickly as possible to ensure service disruption is minimized. If this requires additional resources, Iron Bow will enlist the support of existing staffing partners (Softworld, Metro, Eliassen) who are under contract and ready to support. For Major Incidents not covered under standard support Services, Iron Bow will utilize the T&M rate card (Exhibit 4.1) to acquire temporary resources at VITA's direction in the event of a Major Incident, Problem, or Event to restore Services to the normal state.

16. Provide, install, implement, and configure any tools necessary for the execution of the Services in accordance with the SMM and VITA Rules.

Iron Bow will utilize the following tools for the delivery of EUC:

Table 2 Iron Bow's Solution Tools

Iron Bow Systems to Support Customers	Iron Bow Systems to Support PMO
Cherwell Service Management	Cisco CUCM/Unity
Cherwell Asset Management	Cisco Jabber Client
Microsoft Deployment Toolkit (MDT)	WebEx
Microsoft System Center Configuration Manager (SCCM)	Microsoft Office 365
[redacted]	Microsoft Exchange
[redacted]	Microsoft Windows Server Update Service (WSUS)
[redacted]	[redacted]
[redacted]	[redacted]
[redacted] Backup and Recovery Software	

Iron Bow selected these tools based on current experience, the ability of the tool to integrate easily with the MSI's toolset, and flexibility and scalability across platforms.

While other tools may be used within EUC, Iron Bow understands that the single point of truth will remain with the MSI's SMS. Iron Bow will work diligently to ensure the proper interfaces are designed and working as intended for bidirectional, one directional, real-time, or batch uploads – as determined appropriate/required by VITA and the MSI.

17. Provide end-to-end support for all EUS on VITA-approved End User Devices.

Iron Bow will provide superior delivery of Services to Customers throughout the Device lifecycle as described in this contract which includes all items outlined within Exhibit 2.1. Iron Bow's Service offerings apply to legacy devices, new Devices and Device offerings which may come into scope (ex: through Catalog additions or Agency purchase) throughout the contract duration. Iron Bow's service delivery strategy is based upon a "Customer

first" mantra. Supporting that mantra, is Iron Bow's belief that valuing the employees who deliver those services and providing them the resources they need to do the job will result in achievement of Iron Bow's objectives.

Iron Bow will provide desktop support technicians that are primarily responsible for fixing and maintaining the Commonwealth desktop computing environment used by Customers. Iron Bow will provide assistance remotely (e.g. via the telephone and LAN) as well as via trips to Customer site locations. Iron Bow's field service technicians' common duties will include setting up accounts, repairing or replacing faulty software & hardware, and configuring network settings. Iron Bow technicians will also work together with hardware or software vendors, the MSI, as well as all other STSs to address problems beyond the scope of regular Device maintenance. Iron Bow support technicians will perform all tasks as outlined this contract.

Iron Bow will efficiently provide end-to-end support by using a variety of methods, which includes:

- Separate Resource Units (RUs) for services
  - Ability to support non-Supplier owned Hardware
- Providing tools such as Cherwell Service Management (mobile/tablet application) to close tickets, enter Knowledge Management articles while in the field
  - Includes providing MI-FIs, mobile Devices (tablets or phones) for connectivity
  - Improves SLA for Time-to-Resolve
  - Increases number of tickets Field Service Technicians can respond to by increasing efficiency
  - Expedites escalation
- Leverage collaboration tools
  - Smart Hands - Using Cisco Jabber and Instant Message (IM) improves the interaction between the Field Service Technician and the Service Tower Supplier
  - VIP – Using Cisco Jabber and IM to communicate with Iron Bow SMEs, as needed to resolve VIP issues
- Offer 'Chat' option through [redacted]
  - Integration with Cherwell to generate prompt ticket creation upon chat initiation
  - Reduces travel cost for Field Service Technicians
  - Improves/offers different alternatives for Smart Hands and VIP support
- As a value added offering and in addition to the other support services described herein, Iron Bow will provide walk-in services

  Our solution includes facilities across a number of locations across the Commonwealth. This includes:
  - Chantilly, VA (Iron Bow CSC)
  - Richmond, VA (Iron Bow PMO and Imaging Lab)
  - Henrico, VA (Depot/Asset Disposal)
  - Roanoke, VA (Depot/Asset Disposal)

Iron Bow will establish "walk-in's" or by appointment service hours where technicians will be on-site to assist the User. Services will include but will not be limited to

- While-you-wait diagnostics and repair
- Asset turn in
- PC Refresh
- Password resets assistance
- Access to a printer and copier (Richmond and Roanoke only)

- Hoteling with network access (Richmond and Roanoke only)

Hours will be identified that best supports the User community around the specific location.

18. Support variety of platforms such as Apple, Microsoft, and other Operating Systems (OS).

Iron Bow's solution includes Apple, Microsoft and other Operating Systems (OS). The technology refresh process, as documented in the SMM, will be used to add new platforms if requested by the MSI or VITA in the future. Detailed specifications for each RU are provided in the RU description (see Exhibit 4.2).

Iron Bow's support model includes skilled Field Service Technicians for all platforms. In determining the appropriate vendor certifications (e.g., Dell, HP, Microsoft, Apple, or Android) Iron Bow will survey the User population and the Hardware and Software in use. Iron Bow will align support based on those needs, ensuring Field Services Technicians hold the certifications to best support the Users. For example, Iron Bow will assess where the Microsoft Surface, Mac, and Android Users are located and ensure the EUC Field Services Technicians holding those certifications are staffed in that region. Iron Bow will post in the MSI's Portal, as well as within the Knowledge Management Base within Cherwell (as integrated with the SMS), a listing of certifications held by all of EUC technical staff, as well as Iron Bow's SME resources.

19. Perform requirements gathering for all activities as defined in the SMM.

Iron Bow will utilize several methods including interviews, questionnaires, and observation techniques, to perform requirements gathering in accordance with the procedures outlined in the SMM. Data gathering workshops will be used to rapidly pull together a set of requirements. Workshops will be facilitated and thoroughly planned to achieve the desired results.

20. Support piloting of new End User Devices, Software, and other related services.

Before deploying new End User Devices, Software or other related services, Iron Bow will conduct testing in the lab and will conduct a pilot deployment, if required by VITA. Once testing is completed in the lab, Iron Bow will select a limited number of participants to serve in the pilot. The goal of the pilot program is to examine ease of use and further test and refine deployment strategies and configurations in everyday use prior to full scale production. The results of the pilot installation provide the basis for developing a final plan for deploying new End User Devices, Software or other related services to Users. To finalize the deployment plan, Iron Bow will incorporate feedback from pilot program participants, determine the time and resource requirements for final deployment, and update any documentation, as applicable. Testing will be coordinated with the MSI, in addition to other STS as required.

21. Support testing of Services over VITA-approved network connectivity (e.g., wired, wireless, and remote).

Upon having the appropriate permissions/access, Iron Bow will support testing of Services over the VITA network. Typically, this will be performed on an isolated segment to maintain control. Testing will be coordinated with the MSI, in addition to other STS as required.

2.1.1 Installations, Moves, Adds and Changes (IMACs)

1. Provide IMAC services at in-scope agency locations.

IMACs cover day-to-day activities associated with the scheduling and installation of Hardware and Software, changes to configuration, and de-installation and relocation of equipment, including connectivity testing, data transfer and User orientation. Iron Bow's IMAC service may be a "Hard" or "Soft" IMAC, meaning a Field Service Technician may have to come on site and physically touch the Device to complete the work (Hard) or the Field Service Technician can remotely complete the IMAC service (Soft). Both types of IMACs are performed by the EUC Field Service Technicians in accordance with established SLA's and are conducted with minimum disturbance to the day-to-day operation of business. Iron Bow will perform all IMAC's as a part of the Services.

Iron Bow will work with VITA to define and document each component of Installs, Moves, Adds and Changes included as part of this agreement. Iron Bow Services will include, but may not limited to:

Install: Unpacking and connecting the new system; attaching peripheral Devices that are part of the supported products; performing manufacturer's standard installation tests to verify that the Hardware and Software are functional with network connectivity.

Move: Disconnecting current system units, including the directly attached peripheral Devices; packing equipment to move from existing location to new location; unpacking and reconnecting the same system unit and the directly attached peripheral Devices at the new location; verifying that the Hardware and Software are functional with network connectivity

Add: Hardware - installing an additional external Device and appropriate Device driver to a currently installed system unit; verification through testing upon completion. Software - installing Software products, to a currently installed Device; verification through testing upon completion.

Change: Hardware - performing system modifications for functionality such as a Hardware upgrade or a downgrade with verification testing to ensure Hardware and Software are functional with network connectivity; Software - performing a modification to existing Software or customizing an application load with verification testing to ensure Hardware and Software are functional with network.

IMACS (Soft and Hard) 20 and under Requests for the Same Change Type: IMACs up to and including 20 changes of the same type (e.g. all requests are for the installation of an end user Device for any individual Customer, all requests are to move an end user Device for any individual Customer, and other similar requests for IMACs up to and including 20 end User Devices for any individual Customer) are included in the Services at no additional cost. The IMAC request will come to Iron Bow as a Service Request through the SMS into Cherwell. The Regional Manager will assign resources to execute the IMAC in accordance with the agreed-to SLAs. Once the IMAC is completed, the ticket will be updated in Cherwell (integrated with the SMS).

Project IMACS (Soft and Hard) Over 20 Requests for the Same Change Type): For all IMACs that are over 20 changes of the same type (e.g. all requests are for the installation of an end user Device for any individual Customer, all requests are to move an end user Device for any individual Customer, and other similar requests for IMACs for over 20 end User Devices for any individual Customer) and excluding managed service requests, the IMAC request will come to Iron Bow via one of the following methods:

a. Direct request via the VITA Service Owner
b. Service Request, which may include project requests

For all Project IMACs (Soft or Hard), Iron Bow will include at a minimum:

a. Assigned Project Manager
b. Technical review or requirements completed jointly with Customer
c. Planning and scheduling completed jointly with Customer
d. Reporting and IMAC status notices

Pricing for Project IMACs (Soft and Hard) will be developed based on the technical review, which will be used to determine level of effort. A price proposal, developed using the rate card (Exhibit 4.1), will be delivered to the Customer, as coordinated with the MSI. The price proposal will include each rate proposed, the role title, number of proposed hours, and schedule. Once approved by the Customer, the Iron Bow Regional Manager will assign resources to execute the IMAC. Once the IMAC is completed, the ticket will be updated in Cherwell, as integrated with the SMS.

2. Provide all installations, de-installations, system access, cascades, moves, adds, upgrades, configuration changes and changes for Hardware and Software in accordance with the SMM and VITA Rules.

Any changes will be made in accordance with SMM and VITA Rules. See also Section 2.1.1 #1 directly above.

3. Coordinate, plan, and schedule all IMACs in accordance with the SMM and VITA Rules.

Iron Bow will prioritize IMACs like any other Service Request received through the MSI portal to Iron Bow's Cherwell SMS Ticketing System and carry out the IMACs in accordance with SMM and VITA Rules/processes. See also Section 2.1.1 Installations, Moves, Adds, Changes, #1 above.

4. Test the equipment, Software, and related Services after the implementation of the IMAC to ensure proper function and connectivity (e.g., network access, file open and print capabilities, remote connectivity, Internet/intranet access), in coordination with the MSI.

Iron Bow's Field Service Technician staff will complete the request for IMAC services and validate the installed, moved, added, or modified Hardware/Software is performing as intended. Iron Bow will coordinate with the MSI as appropriate.

5. Provide desk-side orientation relevant to the Users receiving the IMAC.

Upon validation that the installed, moved, added, or modified Hardware/Software is operational, Iron Bow technicians will provide an orientation of the Device or overview of the new functionality. See also Section 2.1 #5 for additional training.

6. Establish and support process to expedite IMAC requests in coordination with the MSI.

Communication will be key between Iron Bow and the MSI, EUC, and other STS. Through prioritization, Iron Bow will plan and track each request for service to meet designated SLAs, as well as expedite through assignment of severity level. The original analyst within the Service Desk will retain ticket ownership, perform follow-up, and monitor while in close communication with the Field Service Technician.

2.1.2 Supplier Personnel

1. Provide personnel that are adequately trained and have appropriate technical skills and competencies to provide support for the Services in accordance with the SMM and VITA Rules

To meet the stated SLAs and achieve a high level of customer satisfaction, Iron Bow will hire individuals who meet the requirements of the specified position. To provide the appropriate level of technical skills and competencies, Iron Bow has assigned minimum requirements to each labor category. Iron Bow will re-badge those incumbent personnel who are performing well under the incumbent contract. For any position where there are new industry or manufacturer certifications, incumbents will be given an adequate amount of time, based on their workload, to achieve the new requirements.

Iron Bow has assigned the minimum certification requirements based on Iron Bow's experience in providing similar technical support. Table 3 below provides a sample of the minimum years of experience by position. The balance of the labor category positions and requirements are in Exhibit 4.1 rate card (Tab 10).

Table 3 Minimum Requirements for PC Desk-side Technicians

Labor Category	Function	Min Years Exp. in Role	Preferred Certifications / Skills
PC Deskside Technician 0	PC Refresh	0	Experience supporting desktop/laptop systems; deploying and disposal of Devices
PC Deskside Technician 1	Field Service Technicians	2	OEM Certs (i.e. Dell Certified Technician, HP Inc Certified Repair); Experience repairing computers and performing technical and system diagnostics as required

PC Deskside Technician 2	Field Service Technicians	4	OEM Certs (i.e. Dell Certified Technician, HP Inc Certified Repair); Experience repairing computers and performing technical and system diagnostics as required
PC Deskside Technician 3	Field Service Technicians	6	A+; OEM Certs (i.e. Dell Certified Technician, HP Inc Certified Repair); Experience repairing computers and performing technical and system diagnostics as required
PC Deskside Technician 4	Field Service Technicians	8	A+; OEM Certs (i.e. Dell Certified Technician, HP Inc Certified Repair); MCP or equivalent, Experience repairing computers and performing technical and system diagnostics as required
PC Deskside Technician 5	Field Service Technicians	10	A+; OEM Certs (i.e. Dell Certified Technician, HP Inc Certified Repair); MCP or equivalent, Experience repairing computers and performing technical and system diagnostics as required

During the incumbent hiring process, Iron Bow will allow for substitution of additional years of experience or alternate (equivalent) certifications in lieu of holding the minimum required certifications. Any new hires will have the required minimum for years of experience and certifications.

In determining the appropriate vendor certifications (e.g., Dell, HP Inc, Microsoft, Apple, or Android) Iron Bow's Transition Team will survey the User population and the Hardware and Software in use. Iron Bow will align support based on those needs, ensuring EUC Field Services Technicians hold the certifications to best support the Users. For example, Iron Bow will assess where the Microsoft Surface, Mac, and Android Users are located and ensure Field Services Technicians holding those certifications are staffed in that region. Iron Bow will post in the MSI's Document Library, as well as within the Knowledge Management Base within Cherwell (as integrated with the SMS), a listing of certifications held by EUC technical staff, as well as Iron Bow SME resources.

Iron Bow staff supporting EUC will have an Individual Development Plan (IDP) created at hire. This plan documents existing education and training, the requirements for the position held and the plan for meeting those requirements. This includes formal education/training or the attainment of certifications, participation in mentoring or on-the job training activities. The IDPs are maintained by each Iron Bow Manager, in addition to the Program Director and Human Resources staff. IDPs are reviewed during employee performance appraisals to ensure training remains on track. Training related to EUC will be tracked within Iron Bow's Corporate Training Tracking database, as well as reported to VITA and the MSI during Program Reviews.

Iron Bow encourages employee participation in educational programs in order to increase their abilities in their present positions, to prepare them for future positions, to keep them current with new advancements or technologies, or as part of their career development program. To provide an additional incentive to employees to continually develop their abilities, Iron Bow will assist staff with Continuing Education expenses. Tuition assistance is generally limited to $5,000 of eligible expenses incurred per fiscal year, per employee and reimbursed based on grade achieved as follows:

A (+/-) - B (+/-) 100%

C (+/-) 75%

Below a C- 0%

Additionally, employees who wish to increase their knowledge in a professional area related to their career can apply for professional development assistance. Assistance is provided for expenses incurred for registration, books, tests/exams, equipment, and supplies required for an approved seminar, course, or certification. Iron Bow will also pay for professional association memberships.

For EUC, all Managers will be required to certify in ITILv3 Foundations. ITIL will help Iron Bow's EUC Managers ensure that there is consistency and predictability in service delivery across their teams, the organization as a whole, and within their processes. ITIL will enable Iron Bow to:

- Provide predictable service level

- Improve efficiency
- Enable consistency in processes
- Perform improved risk management
- Institute effective change management

Incumbent managers will have 6-12 months to achieve ITILv3, depending on work schedule and any other training commitments.

2. Provide personnel that meet Customer-specific background requirements and have completed Customer-specific training.

Individuals assigned by Iron Bow to this contract will meet the VITA and Customer-specific background and training requirements. Iron Bow's recruiting process includes conducting pre-screening against such requirements to ensure candidates comply. Iron Bow's Transition Team will ensure that incumbent personnel who will be re-badged are in compliance with VITA and Customer-specific background requirements and training. Iron Bow's Facility Security Officer (FSO) will maintain information regarding any individual's clearance/access. Additionally, the FSO will work with VITA and the MSI to ensure any information needed on Iron Bow's personnel is communicated according to their processes. For example, in accordance with the MSI's solution, Iron Bow will enter all the required employee information into their Security Clearance System via the portal.

3. Where reasonably practical or as directed by VITA, provide personnel that are dedicated to VITA and are not supplying services to multiple clients of the Supplier.

In most instances, Iron Bow EUC personnel will be dedicated to VITA. Exceptions may include the assignment of temporary personnel required to perform under this contract. These personnel may not be dedicated 100% to VITA. Such time and material resources will only be billed for services performed for VITA. Iron Bow will comply with VITA Rules for any staff assigned to perform the Services. All other resources will be dedicated to VITA as described in Exhibit 5.2.

4. Seek to transition existing personnel or perform appropriate knowledge transfer to ensure knowledge continuity from existing Environment.

As previously stated, Iron Bow will work to re-badge incumbent personnel who are performing well in support of VITA. Hiring incumbent personnel provide continuity of service, particularly during Implementation and will also assist in training any new hires on standard operating procedures (SOPs)/processes. Our ability to hire incumbent personnel is vital for a successful transition as they will be more knowledgeable about the Customer's Environment, and have the ability to share information on business processes, operations, applications, architecture, configuration and tools.

5. Keep Supplier personnel training up to date.

Iron Bow will maintain records on all EUC personnel for any training. These training records will be maintained by Human Resources as part of the employee personnel file. For manufacturer training that results in a certification, Iron Bow's Partner Alliances organization will also track and notify the EUC Program Director and the employee prior to expiration. This will allow the employee ample time to renew.

6. Provide documentation and proof of training and certification to VITA upon request.

Iron Bow will provide documentation and proof of training and certification to VITA upon request.

7. Provide service Personnel who are fully trained and certified by the OEM in direct Support of their product(s) and Device(s).

To meet the stated SLAs and achieve a high level of customer satisfaction, Iron Bow will hire incumbents or new hires who possess OEM certifications to directly support products and Devices. To provide the appropriate level

of technical skills and competencies, Iron Bow has assigned minimum requirements to each labor category. In determining the appropriate vendor certifications (e.g., Dell/EMC, HP, Microsoft, Apple, or Android) Iron Bow will survey the User population and the Hardware and Software in use. Iron Bow will align support based on those needs, ensuring Field Services Technicians hold the certifications to best support the Users. As a Dell/EMC, HP Inc, Apple, and Microsoft certified partner, Iron Bow has access to comprehensive training, tools and support. For HP Inc and Dell, for example, Iron Bow received training credits which will be used to support this contract. For those already being certified – either incumbents or new hires – Iron Bow will work with OEMs to transfer their numbers to Iron Bow (or partner company). Our Partner Alliances Team will work with their counterparts within the channel to accomplish this transfer.

2.2 Field Services and Technical Support Services

1. Provide field services support for End User Devices at VITA Sites

Iron Bow Field Services support will include the following:

- Provide technical support and training to Personal Computer (PC) and PC network Users
- Assist Users in solving problems using available Hardware and Software tools
- Support, install, and maintain PCs, Hardware, OS, Software, and related IT sanctioned peripherals. Install and support both Hardware and Software components for User groups
- Perform preventive maintenance, test and repair of equipment.
- Evaluate system configuration and Software to ensure effective use of Hardware resources. Address and resolve Hardware, Software and Customer issues.
- Engage Users to determine their potential future business requirements.
- Provide positive customer experience with each customer interaction.
- Apply knowledge of processes and resources required to perform analytical and technical tasks on PC systems

There are approximately 105 incumbent personnel currently employed across 3 areas under the supervision of District Managers. Of that population, there are a concentration of those at or nearing retirement. During Implementation, Iron Bow is prepared for some incumbent personnel to stay with their current employer or change jobs/careers. There are a number of strategies Iron Bow will put in place to mitigate losing this corporate knowledge. Iron Bow's strategies include, but may not be limited to the following:

Iron Bow has letters of commitment from 4 existing incumbent senior leaders. Iron Bow has discussed compensation and benefits and will hire these individuals immediately upon Effective Date. Our named Program Director has already been hired in order to leverage his knowledge and ability prior to award. Through the Program Director and the other incumbent leaders, Iron Bow believes those incumbent Field Services Technicians who were reluctant to transition due to fear of change, will now stay. Iron Bow's solution accounts for hiring incumbent Field Services Technicians at an equal or better rate of pay and caliber of benefits. Additionally, Iron Bow will offer incentives to those in the retirement zone should they elect to stay. Incentives include, but are not limited to sign on bonuses, alternative employment arrangements such as 1099, or grandfathering paid time off accrual rates.

During Implementation, Iron Bow's Transition Team will quickly perform an assessment of the incumbent population to determine the number of vacancies. Iron Bow's dedicated Recruiting Team is already building a database of candidates. Iron Bow will begin screening candidates upon notification of selection in order to begin interviewing once vacancies have been identified. These activities ensure Iron Bow is at full strength upon Commencement and will cause no degradation in Services to End Users.

Additionally, immediately after award, Iron Bow will be performing an assessment of individual performance, location, and operational policies. The Transition Manager and other members of Iron Bow's Transition Team (e.g., Quality Assurance and Training) will shadow Field Service Technicians to understand workflow, processes and policies in place, and their level of skills and ability to perform their duties. Once Iron Bow has this information, territory coverage, processes and workflows, and skills will be documented. This will allow Iron Bow to validate any information being provided by the incumbent as well as gets Iron Bow out in front of personnel to alleviate any concerns they have with respect to Service takeover and Implementation.

Field Services Technicians will either sit at an Agency (per Agency request and available space) or work remotely from their vehicle from a home base. In the short-term, Iron Bow will utilize any space available for Field Services Technicians under the "take over in place" strategy. Additionally, Iron Bow and our partners have a number of facilities across the Commonwealth where Field Services Technicians will use office space as needed. Iron Bow will utilize Field Services Technicians to support on other activities, such as PC Refresh where needed.

2. Provide break/fix Software and Hardware support (including OEM-certified warranty repairs) in accordance with the SMM and VITA Rules.

As part of Iron Bow's managed Service model, break/fix Hardware and Software support will be provided as described herein and in accordance with the support level (e.g. VIP, gold, silver, bronze) selected for the Device. When an issue occurs, an Incident Request is submitted by End Users through the MSI Portal into the SMS ticketing system. A Tier 1 Service Desk technician will escalate to a Field Service Technician who will triage and then diagnose the issue, first remotely and then at the desk side as needed. The Field Service Technician will escalate to Tier 3 or to another STS in accordance with documented Escalation Procedures found in the SMM and as needed. If an issue requires replacement, Iron Bow will coordinate with the manufacturer as needed through resolution. As an HP Authorized Repair Partner, Iron Bow has access to vendor-certified resources to support EUC on-site personnel to resolve the most difficult issues. Upon resolution, Iron Bow will log how the issue was resolved in Cherwell (as integrated with the SMS). Additionally, log information or a draft Knowledge Article will be created and made available to help the technicians resolve issues more quickly if they occur again. For Problems, known errors will be documented in the Known Error Database.

3. Perform asset disposal in accordance with the SMM and VITA Rules.

Iron Bow will provide asset disposal for the Hardware included in the Iron Bow Services under this Contract. This includes both legacy Devices and Devices issued by Iron Bow. Iron Bow's asset disposal process will ensure Devices are dispositioned properly and securely at the end of their lifespan/use, thereby minimizing risks including the unauthorized release of confidential data and/or information, the violation of Software license agreements, and unauthorized disclosure of intellectual property that might be stored on the Devices. Iron Bow's asset disposal processes for this contract will comply with VITA Rules.

For asset disposal, Iron Bow will team with Core Technologies (Core), who are currently performing asset disposal for the Commonwealth. Core has created and will use a comprehensive procedural guide that documents the disposal process. Through the subcontractor relationship with Core, Iron Bow will provide a paperless process with emailed pick up receipts and electronic signatures, in addition to creating a mail in disposal process for small quantity pickups, which will be included in the SMM.

Iron Bow will provide a smooth transition of Service to ensure there is not a buildup or back log of end of life assets at Agency locations. Additionally, through the subcontracting relationship with Core, Iron Bow will also create efficiencies to streamline the current process disposal process. Iron Bow will provide goods and services including:

- Technicians will be empowered at the time of refresh to pack and prepare assets for disposal, hence reducing the time between asset refresh and asset disposal
- Technicians will be equipped with barcode scanners to expedite service and reduce data errors
- Refresh Team and Disposal Teams will work in unison by sharing information such as refresh schedules, forecasts and Agency initiatives which will assist in planning asset disposal
- The Refresh Team and Disposal Teams will be given access to on-line tools to update tickets at time of Service for better tracking and updated ticket data will be made available to Customers
- Historical data on assets will be generated via Cherwell and interfaced with the MSI tools

End Users are not to dispose of the Hardware included in the Iron Bow Services under this Contract on their own. In the case that an End User disposes of Hardware on their own it will be handled as a Lost or Accidentally Damaged device as described in Exhibit 4.2.

Asset Disposal Processes

The Iron Bow Asset Disposal Team Lead and/or Project Manager will oversee asset disposal operations and develop quality assurance benchmarks that will be continuously reviewed by the Iron Bow Program Director and Quality Assurance (QA) Team. These benchmarks include but are not limited to:

- Timeliness of services delivered
- Accuracy of data
- Value to Customer
- Approach to problems
- Responsiveness to Customer
- Customer Relationship

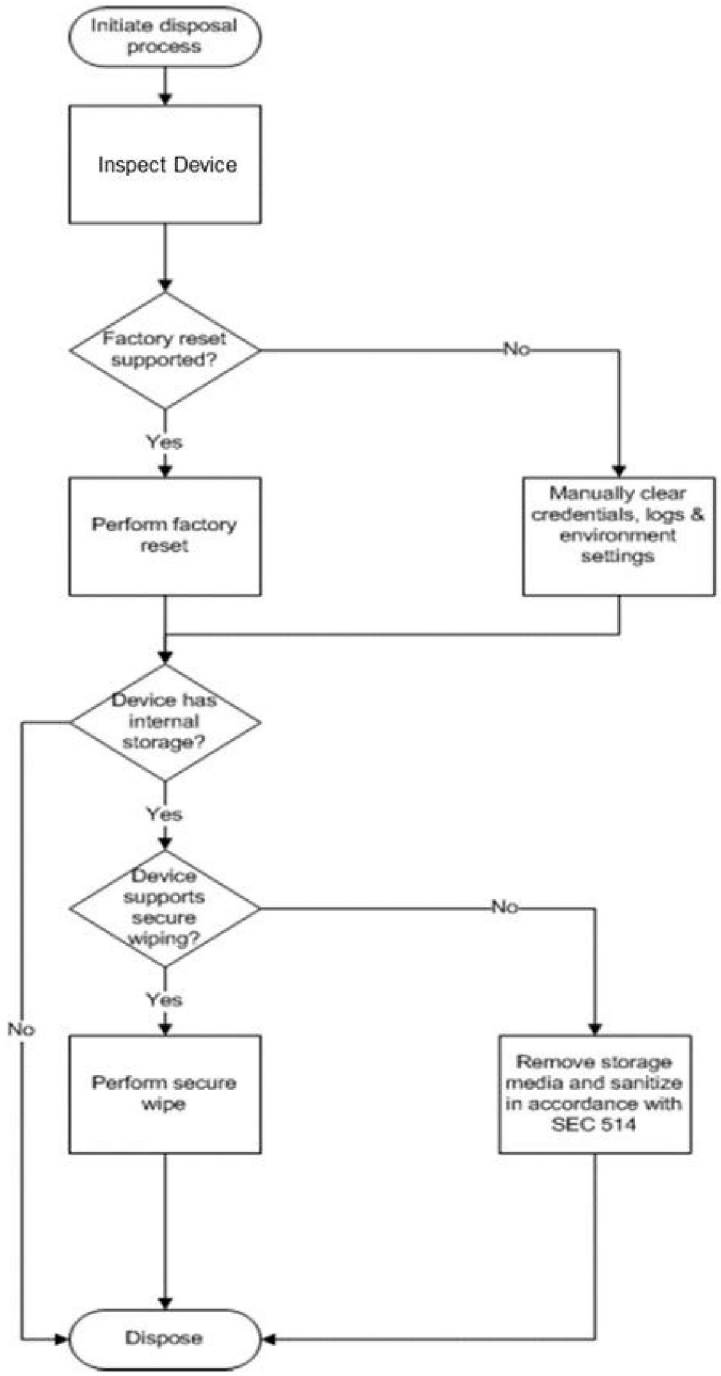
The Iron Bow QA Team and PC Refresh Team Managers as well as the Asset Disposal Team will audit asset disposal processes quarterly. Leads will meet weekly to discuss schedules, forecasts, special projects, challenges, efficiencies and new initiatives.

Iron Bow's Information Technology Asset Disposal (ITAD) services will consist of standard and enhanced Services:

- **Standard Information Technology Asset Disposal Services** are the disposal of desktop computers, laptops, tablets, and all related accessories and miscellaneous components for the Hardware included in the Iron Bow Services under this contract. This includes both legacy Devices and Devices issued by Iron Bow. Iron Bow will provide standard ITAD services for both early refreshes and regularly scheduled refreshes.
- **Enhanced Information Technology Asset Disposal Services** include options for both Agencies and other STS to purchase disposal services for additional Agency or STS owned assets that are not included in the standard ITAD services. This may include "clean outs" of stored assets, secure transports and disposal of other equipment such as mainframes, storage arrays, personal digital assistants (PDAs), all network related equipment, all storage media, all phone Devices, printers, multi-function Devices (MFDs), all external storage Devices and any other VITA or Agency owned IT equipment. Iron Bow will provide removal of assets from the site, proper data removal (as appropriate for the asset type), certification of data removal, data removal quality assurance (QA), chain-of-custody services (where required), and transfer of ownership (where required). Iron Bow will provide on-site data destruction as requested. All enhanced asset disposal services will be billed as described in Section 4.4.1.

- Also as an enhanced asset disposal service, Iron Bow will make an Asset Management Technician available for miscellaneous services and special projects as needed on an hourly basis at the rates described in Exhibit 4.1.

Methodologies and processes for asset disposal will be developed using VITA ITRM Standards in accordance with the VITA Rules and a high-level draft of the process is summarized below:



Stage 1 - Initiate Disposal Process

Standard ITAD Services will be managed by Iron Bow as part of the refresh process. When a device is refreshed, Iron Bow will remove the Customer's current Device at the same time as the installation of the new Device. If the asset reaches EOL/EOS and the Customer choose not to refresh the Device, Iron Bow will coordinate the return of the Device with the Customer within 30 days of the end of the asset's removal from service.

Enhanced ITAD Services will be initiated by a Service Request through the MSI Portal in the SMS. A Consolidated Asset Disposal (CAD) form will be completed and attached to the ticket. A detailed list of the assets to be picked up, ticket number, details on the POC and Agency information must be included on the CAD form. Iron Bow will coordinate the return of the Device with the Customer and the return process will be by mail in or pick up as described below.

- **Optional Mail In Process:** If there are five (5) or less assets, an asset mail in process will be offered to the Customer. Iron Bow's Asset Disposal Team will provide all packing materials and a prepaid shipping label for the return of assets. The Customer will pack up the equipment and stage for a pick up and transport to one of the depots. A copy of the CAD form must be included in the shipment for processing. Iron Bow will receive and process all assets associated with mailers within seven (7) calendar days of receiving the ticket. Updates noting status of delivery will be tracked in the ticket for Customer review and reporting.
- **Asset Pick Up Process:** For asset pick-ups of six (6) or more assets or for large equipment, the Asset Disposal Team Dispatcher will receive the Service Request and review for special instructions and determine resources needed. The Dispatcher will contact the POC via email and/or phone call to schedule the asset pick up. If the POC is unable to be reached within 5 days, which will include at least 3 contact attempts during the period, the Dispatcher will escalate to the Iron Bow Program Director or appropriate District Manager to confirm POC information and assist in scheduling asset pickup. Once a scheduled pick up time and date are established, the Asset Disposal Team will prepare the pick-up instructions for the disposal technician. These instructions will note the assets that are authorized to be picked up with specific instructions on method of transportation needed to secure assets with data. Only assets noted on the CAD form will be removed from the site and, as a receipt, Customers will be provided a copy of the pick-up ticket. Iron Bow will pick up and process all assets within 10 calendar days of receiving the ticket. Updates noting scheduling and Device pick up will be tracked in the ticket for Customer review and reporting.

Customers will be provided with an electronic copy of the chain of custody documentation, as required. Iron Bow will follow VITA Rules to maintain the chain of custody when picking up assets and transporting them from an Agency site. The chain of custody form will include the following information:

- Serial# of asset being removed
- Asset Tag# of asset being removed
- Number of total assets being moved
- [redacted]
- [redacted]
- [redacted]

- Dated and signed by the observing Customer designated POC

Stage 2 - Receiving Assets and Data Destruction

Iron Bow's Asset Disposal Team will transport the Devices to one of the Iron Bow depots. Upon arrival the chain of custody seals will be broken and Devices will be verified and scanned, as applicable, into the Cherwell Asset Management System, which will be integrated with MSI's CMDB. Iron Bow will, unless otherwise directed, wipe the Device within 48 hours of receipt. As a secondary source of security, Devices, including those that are mailed in, are stored in a secure caged area until the data destruction process has been completed.

Iron Bow's Asset Disposal Team will overwrite the Devices using [redacted] whenever possible. [redacted] will be utilized for all SSD media. When it is not possible to use an overwrite or encryption process or the overwrite process fails, Iron Bow's vehicles and depots are equipped with, and Iron Bow will use, piercing devices for physical drive destruction. Iron bow will use the Clear/Purge process as outlined in VITA Rules for data destruction on Apple Devices.

Iron Bow will utilize a minimum of two (2) depot facilities to support ITAD.

Depot Facility – Located in Richmond, VA (Henrico)

This depot currently provides the following ITAD services in support of the current contract and will continue to do so as part of Iron Bow's Services:

Features:	**Equipped with the following:**
• Scheduling and Logistic Services	• 24-hour security monitoring system
• Secured Pick-ups using Chain of Custody Process	• A secure technical lab for wiping and imaging up to 250 assets at one time.
• Data Destruction (on customer site and in at depot)	• A fleet of transportation vehicles to handle large and small projects
• Asset Tracking and Reporting	• GPS Tracking System on all Vehicles
• Asset Re-location and moves	• 4,000 sq. ft. of Warehouse storage for processed assets
• Support of Special Projects.	• A caged area for secure storage of assets with data, holding for customer direction

Additional Depot Facility – Located in Western VA (Roanoke)

Iron Bow will add a second depot facility in the Western region of Virginia, preferably Roanoke. By adding this location, Iron Bow will be able to reduce travel time and the lead time on picking up assets on this end of the state. This facility will serve the same functions as the Richmond Depot:

- Scheduling and Logistic Services
- Secured Pick-ups using Chain of Custody Process
- Data Destruction (on customer site and in at depot)
- Asset Tracking and Reporting
- Asset Re-location and moves
- Support of Special Projects

Iron Bow will also incorporate some new capabilities at both of Iron Bow's depot locations. Such capabilities will include but may not be limited to storage of hot swappable Devices and spare parts harvesting. Iron Bow will also gain space for repairs and a home base for some of Iron Bow's Smart Hands Technicians and Engineers.

Areas where Devices are staged for sanitization will be secure and only accessible by properly cleared staff and will not contain other inventory.

Stage 3 - Disposal

After data destruction, Devices will be disposed of in one of the following ways:

- Iron Bow will return or dispose of leased assets that have reached the end of their term in accordance with the terms of Iron Bow's lease agreement(s) so long as such terms do not conflict with the VITA Rules or any other terms and conditions described herein.
- Iron Bow will transport Agency owned assets to DGS facilities as is required by the Customer. Asset tags for Agency owned assets will remain for tracking and processing at DGS facilities. Agency owned assets will be separated and stored in a specific designated area until they are transported to the DGS facility.
- Iron Bow will otherwise destroy and dispose of the asset in accordance with VITA Rules.

Iron Bow will use reasonable efforts to recoup any residual value of the disposed asset whenever possible. Any value that Iron Bow recoups from the sale of a disposed asset, in whole or in part, will be returned to VITA in the form of an invoice credit on a monthly basis.

Asset Disposal Data Collection and Submittal

Iron Bow will capture and maintain the following information on the data destruction and disposal of Devices:

The Asset Disposal Team will process a weekly Certificate of Destruction documenting the following information:

- COV agency name
- Address of asset
- Serial number of chassis
- Asset Tag number whether Incumbent, Agency or VITA tags
- Vendor organization or 3rd party performing data removal operation
- Name of person performing removal
- Equipment type (laptop, desktop, tablet, server, NAS, etc.)
- Date of overwriting or data removal
- Method used for data removal
- Printed name and signature of the person's supervisor

The Asset Disposal Team will perform Quality Assurance (QA) checks on recovered and destroyed Devices as is required in the VITA Rules. Iron Bow will document information such as but not limited to:

- Serial number
- Date QA was performed
- Printed name of the tester(s) who performed QA
- Total number of Devices QA tested
- Method of testing to ensure data removal
- Results of testing (what were the results of the testing method)
- Confirmation that the asset tag and any other non-manufacture identifiers are removed

The Asset Disposal Team will provide weekly and monthly asset disposal reports that will include but are not limited to the following information. Additional fields of information will be added per VITA's request.

- Ticket Number
- Date of Pick up
- Serial Number
- Asset Tag Number
- Method of Data Destruction
- Date of Destruction
- Asset Type
- Asset Final Disposition
- Agency Location

Copies of all Data Removal Certification, QA checks, and Chain-of-Custody documents will be provided to VITA within 15 (fifteen) business days of removal of the Device from the site. Signed documents will be provided in .pdf format with a standardized naming convention, and will be delivered via a web-based portal. Month end reports will be rolled up into a "living list" of all assets processed for Customer review.

4. Provide field services support training on new products and services as they become part of the Supplier's responsibilities; provide proof of training as requested

Iron Bow will maintain the technical skills and vendor certifications for the Field Services Support technicians because it is critical to Iron Bow's consistency in meeting the SLAs and achieving a high level of customer satisfaction. Relationships with HP, Dell, Apple, and other top tier manufacturers enable Iron Bow to receive advance access to training, tools, white papers, and even demonstration equipment that would not be otherwise available. Through these partnerships programs, Iron Bow earns training credits that will be used in support of this contract. As new products or services are integrated into the offerings, Iron Bow will ensure staff receives timely training and provides proof of such training, as requested. Iron Bow will also utilize Tier 3 resources (subject matter experts) on this contract to support any requests from the MSI or Customers for training and to supplement training the Field Services Technicians on new products and Services when needed.

5. Provide support for End Users who are traveling or remotely accessing VITA services (e.g., from home offices), including shipping replacement Devices or leveraging Third Party Hardware repair (or other form of onsite support).

Iron Bow will use [redacted] which will allow Iron Bow to access systems and support End Users easily, while protecting credentials and endpoints from threats. Through [redacted] Iron Bow's technicians will have access to desktops/laptops and critical systems to remotely support End Users anywhere, on any platform. Iron Bow's Field Service Technicians will utilize [redacted] for an improved customer experience. Iron Bow will integrate live chat support with Iron Bow's remote support to meet with customers where they already are – whether travelling, at home, or in the office. [redacted] provides two-factor authentication, advanced encryption, granular permissions, and comprehensive audit trails. Iron Bow's EUC support, depending on the issue, also includes shipping replacement Devices or leveraging Third Party Hardware repair when required.

6. Assist in troubleshooting issues involving business applications on and off premise (e.g. cloud), including evidence that performance problems are not caused by Supplier Services.

Iron Bow's Field Service Technicians will follow a logical and methodical workflow to analyze and resolve issues. To resolve an application issue, Iron Bow will first seek answers to the following types of questions: is it one User or many; one server or several; is it a particular application; when does the issue happen - all the time or at a certain time; does it impact local or remote Users or both; and/or were there any recent changes. The answers to these questions will allow Iron Bow to prioritize based on the number of Users impacted. Iron Bow will then follow a set approach, which is based on common, industry best practices, to troubleshoot the issue which begins with determining if an issue is related to a network, a server, or an application problem. After that

determination is made, Iron Bow will provide a more targeted investigation, analysis, and, ultimately, a resolution. This approach will enable Iron Bow to engage the appropriate resources and tools. Iron Bow's EUC Field Service Technicians will be responsible for troubleshooting business applications; if it is discovered that performance problems are not caused by Services under the EUC Supplier's control or area of responsibility, Iron Bow will assist in the resolution as needed; and the ticket will be re-routed to the appropriate group/Service Tower/MSI.

7. Provide dedicated onsite personnel (i.e., stationed at or near Customer Sites) where requested.

Iron Bow will provide dedicated personnel on the Customer site where requested and space is available. Where space is not available, Iron Bow's Field Service Technicians will provide support remotely from one of Iron Bow's locations in the region and dispatch field service technicians or 3rd party resources (through one of Iron Bow's OEM partners) if the issue cannot be resolved remotely. Iron Bow will provide 3rd party resources in compliance with the VITA Rules.

8. Work with Customer personnel or other supplier staff as may be required to effect resolution, asset management updates, etc.

Iron Bow will routinely work with Customer personnel, other STS staff, and/or the MSI to achieve resolution of issues. As part of Iron Bow's Project Management activities, Iron Bow will establish and publish a Communications Plan to ensure appropriate points of contact are available to work collaboratively across the organization. This includes, among other things, maintaining an accurate, current, and complete inventory of assets and any updates thereto.

2.2.1 Desk-side Support Operations

Desk-side Support Services provide the most efficient path to get – and keep – End-Users connected and productive. Iron Bow's EUC services include, but are not limited to: desktop image development, management and distribution; Hardware and Software vendor management; IMAC and break/fix; desktop application packaging and End User group profile management; Hardware and Software configuration; and data migration.

1. Perform End User Device configuration, imaging (including advisory and technical Support for image engineering and Image distribution), and Application installation, as well as ongoing Patch and driver update testing and distribution.

Iron Bow's desk-side support staff will perform a variety of functions to support End Users. Such functions include configuring Devices, imaging, installing any additional applications and drivers, and ensuring those applications are Patched and drivers updated, accordingly. Iron Bow's processes and tools used for these activities are outlined in Section 2.3 Software Services.

2. Perform End User Device, Operating System, Software, and Application troubleshooting, repairs and, as necessary, restorations.

Desk-side support will be used when troubleshooting more advanced issues that cannot be resolved remotely. Section 2.2 #6 above outlines Iron Bow's process for troubleshooting and diagnosing application/Software issues. See Section 2.2.2 for system restores.

3. Provide the necessary tools to ensure the integrity of the VITA End User Device Environment, efficiently conduct required administrative and operational activities

Iron Bow will provide and use Cherwell IT Service Management, which offers IT workflow. Using the IT workflow automation in Cherwell, Iron Bow will automate repetitive and complex tasks. Iron Bow's instance of Cherwell will be deployed on premise in Iron Bow's Richmond Program Office facility and backed up in a collocated data center (Colo). Iron Bow will integrate Cherwell with the MSI's SMS.

Iron Bow will provide and use Cherwell Asset Management, which is an IT Asset Management (ITAM) tool designed to support large reductions in Software license spending, IT overhead, and Software audit risk. By integrating all the data related to Hardware and Software inventory, application usage, license entitlements, and IT purchases, Iron Bow will have the ability to track and manage IT investments from purchase to retirement. Cherwell Asset Management will be integrated by Iron Bow with Cherwell Service Management and SCCM, populating the Cherwell CMDB with IT asset data, and providing Iron Bow's staff with information needed for effective incident, problem, and change management. Iron Bow will integrate the tools with the MSI's SMS.

Iron Bow will provide and use [redacted] for remote troubleshooting as well as seeking additional support from Iron Bow's SMEs at another location. Through [redacted] Iron Bow's EUC Field Service Technicians will have access to desktops/laptops and critical systems to remotely support End Users anywhere, on any platform.

Images will be built and packaged with MDT and deployed and Patched with SCCM, [redacted] See Section 2.3 Software Services, for the detailed description of Iron Bow will use the tools to provide the Services.

4. Resolve issues remotely where possible, including via remote administration tools (e.g., desktop takeover), in accordance with the SMM and VITA Rules.

Iron Bow will use [redacted] to access systems and support End Users easily, while protecting credentials and endpoints from threats. Through [redacted] EUC Field Service Technicians will have access to desktops/laptops and critical systems to remotely support End Users anywhere, on any platform. Iron Bow will utilize [redacted] chat feature for an improved customer experience. Iron Bow will integrate live chat support with Iron Bow's remote support to meet with customers where they already are – whether travelling, at home, or in the office. [redacted] provides two-factor authentication, advanced encryption, granular permissions, comprehensive audit trails. Iron Bow's EUC support, depending on the issue, includes shipping replacement Devices or leveraging third party Hardware repair when required.

5. Provide onsite Support for Incidents, Service Requests, and Changes that cannot be conducted remotely (e.g., IMAC, break/fix).

No matter the size or complexity of the problem, Iron Bow's certified EUC Field Service Technicians will be deployed on-site to troubleshoot and solve whatever IT issue the User is currently facing. This includes but may not be limited to IMACs (see Section 2.1.1) or break/fix (see Section 2.2 #2).

6. Maintain Support relationships with Software and End User Device OEMs (e.g., Apple, Dell) to ensure timely access to OEM support teams and engineering functions.

Iron Bow will maintain relationships with OEMs that provide access to their subject matter expertise to support resolution of VITA's most challenging issues. Figure 1 below describes Iron Bow's top OEM partners and certification levels which will be maintained during the contract, unless otherwise approved by VITA.

HP Inc- Platinum Certified Partner

HPE- Platinum Certified Partner

DELL EMC

Microsoft
Gold Certified Partner

CISCO
Gold Certified Partner

vmware

Premier Partner, Federal Authorized Solutions Provider Enterprise Partner

Figure 1 Iron Bow's Top OEM Partners and Certification Levels

7. Provide and utilize tools to assist in the diagnosis and Resolution of assigned tickets (e.g., external backup drives, hand and small power tools and diagnostic Software).

When responding to any incident or service request under the EUC area of responsibility, Iron Bow's Field Service Technicians will utilize a variety of tools, diagnostic Software, and spare parts. This includes: hardware diagnostic tools (e.g., LCD desktop & laptop motherboard diagnostic test card), computer PC diagnostic test kits for desktop and laptop computer technicians, and computer diagnostic software tools.

8. Provide tools and capabilities to permit Users to perform limited self-support.

Iron Bow will use the Knowledge Management System to publish self Help, how to guides and frequently asked questions as methods to decrease call volume to the Service Desk. Iron Bow EUC Field Service Technicians will prepare Knowledge Articles to contribute to the Knowledge Base to support self-help. Iron Bow will also utilize EUC Field Service Technicians to conduct User training to provide a good working knowledge to the User.

2.2.2 End User Device Recovery

1. Perform restoration and data recovery in accordance with SMM and VITA Rules.

Iron Bow will perform restoration and data recovery in accordance with the SMM and VITA Rules using one of the following methods. Iron Bow will use similar methodologies for other supported operating systems.

System Restoration. Iron Bow will use System Restore to restore the Windows installation back to its last working state. It does this by creating "restore points." To restore a PC to an earlier restore point, any apps installed after that point will get uninstalled. Apps that were installed when that restore point was created will still be in place. Apps that were uninstalled after the restore point will be restored by Iron Bow. However, since System Restore only restores certain types of files, programs that get restored often will not work, or at least, not work properly until the installers are re-run.

System Restore is different than making a backup. It specifically works on the underlying Windows system, rather than everything on the hard drive. As such, System Restore does not save old copies of personal files as part of its snapshot. It also will not delete or replace any of the personal files when a restoration is performed. System Restore does not work like a backup. Because of this, Iron Bow will always backup data before a system restore.

System Recovery. Iron Bow will also perform System Recovery. Windows 10 includes a "Reset your PC" option that quickly restores Windows to its factory default configuration. It is faster and more convenient than reinstalling Windows from scratch or using the manufacturer's recovery partition. When the "Reset this PC" feature is used, Windows resets itself to its factory default state. All of the manufacturer installed Software and drivers that came with the PC will be reinstalled. There will be an option to keep personal files or erase them. However, all of the installed programs and settings will also be erased. This ensures there will be a fresh system. Problems caused by third-party Software, system file corruption, system settings changes, or malware will be fixed by resetting the Device.

If the computer came with Windows pre-installed, a third option exists, "Restore Factory Settings". This will restore the original version that came with the PC.

2. Reinstall the latest approved and eligible image in accordance with SMM and VITA Rules.

After the system is restored, Iron Bow will reinstall the latest approved and eligible image.

3. Configure the repaired or replacement asset to the configuration of the original (e.g., install Software, drivers, printers, network connectivity, peripherals, locally stored data, etc.) in accordance with the SMM and VITA Rules.

Once the OS is restored or recovered, Iron Bow's technicians will ensure that all of the additional Software, drivers, peripherals, connectivity and data are returned to the prior state. Prior to leaving the desk-side, Iron Bow will check to ensure the User has all of the capability they need to perform their job.

4. Recover data from failed Devices where technically possible, unless directed otherwise by VITA.

The most common data recovery scenario involves an OS failure, malfunction of a storage Device, logical failure of storage Devices, or accidental damage or deletion (typically, on a single-drive, single-partition, single-OS system). In this case, the ultimate goal is to copy all important files from the damaged media to another new drive. Iron Bow will accomplish this by using a live CD, many of which provide a means to mount the system drive and backup drives or removable media, and to move the files from the system drive to the backup media with a file manager or optical disc authoring Software. Such cases are often mitigated by disk partitioning and consistently storing valuable data files (or copies of them) on a different partition from the replaceable OS system files. Full disk encryption makes this a little more complicated but Iron Bow's technicians will still be able to achieve this.

Another scenario involves a drive-level failure, such as a compromised file system or drive partition, or a hard disk drive failure. In any of these cases, the data is not easily read from the media Devices. Depending on the situation, Iron Bow will provide solutions such as repairing the logical file system, partitioning table or master boot record, or updating the firmware or drive recover. Iron Bow will use techniques ranging from Software-based recovery of corrupted data, Hardware- and Software-based recovery of damaged service areas, and Hardware replacement on a physically damaged drive, which involves changing the parts of the damaged drive to make the data in a readable form so that it can copied to a new drive. If a drive recovery is necessary, the drive itself has typically failed permanently, and Iron Bow will focus on a one-time recovery, salvaging whatever data can be read.

In a third scenario, files have been accidentally "deleted" from a storage medium by the Users. Typically, the contents of deleted files are not removed immediately from the physical drive; instead, references to them in the directory structure are removed, and thereafter space the deleted data occupies is made available for later data overwriting. In the mind of End Users, deleted files cannot be discoverable through a standard file manager, but the deleted data still technically exists on the physical drive. In the meantime, the original file contents remain, often in a number of disconnected fragments, and may be recoverable if not overwritten by other data files.

The following process will be followed by Iron Bow EUC Field Service Technicians to recover data in this scenario:

Phase 1 - Repair the hard disk drive. Repair the hard disk drive so it is running in some form, or at least in a state suitable for reading the data from it. For example, if heads are bad they need to be changed; if the PCB is faulty then it needs to be fixed or replaced; if the spindle motor is bad, the platters and heads should be moved to a new drive.

Phase 2 - Image the drive to a new drive or a disk image file. When a hard disk drive fails, the importance of getting the data off the drive is the top priority. The longer a faulty drive is used, the more likely further data loss is to occur. Creating an image of the drive will ensure there is a secondary copy of the data on another Device, on which it is safe to perform testing and recovery procedures without harming the source.

Phase 3 - Logical recovery of files, partition, Master Boot Record (MBR) and file system structures. After the drive has been cloned to a new drive, it is suitable to attempt the retrieval of lost data. If the drive has failed

logically, there are a number of reasons for that. By using the clone, it may be possible to repair the partition table or MBR in order to read the file system's data structure and retrieve stored data.

Phase 4 - Repair damaged files that were retrieved. Data damage can be caused when, for example, a file is written to a sector on the drive that has been damaged. This is the most common cause in a failing drive, meaning that data needs to be reconstructed to become readable. Corrupted documents will be recovered by several Software methods or by manually reconstructing the document using a hex editor.

2.2.3 Cross-STS ("Smart Hands") Support

1. Where Supplier has onsite or local staff, support the MSI, Service Tower Suppliers, and Customers in resolving non-EUS Incidents and issues.

Iron Bow Field Service Technicians will provide Smart Hands support for any issues supporting the MSI, STS and Customers for non-EUS incidents. The Smart Hands will respond on-site and take direction telephonically, through chat, or video (such as WebEx) from the experts who reside in the Service Towers. This makes use of local or on-site resources and does not require the MSI, STS, or Customers to dispatch a SME resource.

Iron Bow will collaborate with the MSI and other STS providers to develop the processes for requesting and delivering Smart Hands services. Any charges for such services will be managed between Iron Bow, the MSI and other STS providers.

2. Coordinate with and support MSI and STS as directed by VITA, the Customer or the MSI, and in accordance with the SMM and VITA Rules.

Iron Bow will coordinate with the MSI and STS to supply Smart Hands. This includes working to schedule resources to fix the issues within the timeframe required. EUC Field Services Technicians supplying Smart Hands will have direct access to Iron Bow SMEs at no additional charge, as needed for more complex issues or those issues involving multiple Users. Field Services Technicians will be provided with a list of SMEs, phone numbers, and emails in the MSI's Document Library or Knowledge Management System.

3. Accept, manage, address, resolve issues affecting the local Devices in the distributed Environment (e.g., printers, network, voice, servers), including IMACs, in accordance with the SMM and VITA Rules.

Iron Bow will accept, manage, address, and resolve issues impacting Devices outside of the EUC area of responsibility. Iron Bow's Field Service Technicians have broad experience across many areas providing them a general level of knowledge. This knowledge, along with the guidance of personnel with domain experience, will provide an effective approach to fixing these problems. The issues will be received, tracked and managed as a ticket within Cherwell.

2.2.4 VIP Support

1. Provide support for VITA-identified VIP Users in accordance with the SMM and VITA Rules.

After Effective Date, Iron Bow's Transition Team will perform an assessment of the End User population to determine how many End Users are currently designated as VIP and where they are located. This will provide Iron Bow with an idea of where the support is currently needed for planning and training purposes. If there are concentrated areas of VIP End Users (i.e. the Office of the Governor), Iron Bow will designate a VIP Team that will provide dedicated Service. After Implementation, Iron Bow will meet with Agencies to determine their needs and adjust the EUC Field Service Technician team composition, accordingly.

Iron Bow will provide expedited support to those End Users purchasing the VIP Support RU. This support includes hands-on, white glove desk-side support. Our VIP support will provide for the resolution of issues and problems from end to end and includes coordination of multiple teams and support personnel as needed to resolve the incident as quickly as possible and meeting or exceeding the 4, 8 or 12-hour resolution time SLA

depending on the VIP's geographical location (as defined further below). Our VIP service is available 24x7x365 and supports VIP work and home Environments for Hardware, Software, network and other technology needs. Liability issues will be discussed with VITA and Customers prior to in-home service being provided. Procedures related to in home service will be submitted to VITA for approval and included in the SMM upon acceptance.

VIP Services are made via Service Request to the MSI portal. Upon receipt of a VIP ticket, the Tier 1 Technician will follow up with a phone call to Tier 2 single point of contact (designated within the SMM) to alert Tier 2 that a VIP Ticket has been logged. The agreed to timeframe for the call will be established as an OLA between the MSI and Iron Bow. The Field Service Technicians assigned to VIP requests are SMEs across multiple components and technologies used including: desktop/laptops/tablets, mobile Devices (Android/iOS), Wi-Fi and LAN connections, A/V Equipment and conference room support, peripheral setup, hard phones & VoIP (e.g. Skype), online conferencing and office productivity software (e.g. O365 Skype Meeting Support, Google G-Suite) within Mac, Linux, and Windows Environments.

VIP's will be classified and business rules and SLAs configured within Cherwell to prioritize requests from VIP users. A VIP process, maintained in the SMM, will detail how a VIP user is handled and transferred from initial contact through the MSI's Service Desk to an EUC Field Services Technician. When a VIP ticket is transferred to Iron Bow within Cherwell, an icon identifying the user as a VIP will appear next to the person's name. This visual indicator will serve as a reminder to the technician to the level of support and response required.

Iron Bow has defined three (3) levels of VIP users based on geographical region, as follows:

VIP Support (Richmond District): Service Requests received for VIP End Users in the Richmond District will be performed in accordance with the SLA's for VIP Support (Richmond District). The Richmond District is defined as any location identified as part of the Richmond Service Area (Zip codes for Richmond District will be defined within the SMM and site list maintained by the MSI). The VIP Service Request will come to Iron Bow through the SMS into Cherwell. The Iron Bow Regional Manager will assign resources to execute the VIP support. Once the VIP support is completed, the ticket will be updated in Cherwell (integrated with the SMS).

VIP Support (Outside Richmond District - Urban): Service Requests received for VIP End Users outside of the Richmond District, but within a designated Urban area will be performed in accordance with the SLA's for VIP Support (Outside Richmond District - Urban). The Outside Richmond District (Urban) designation is defined as any geographical area outside the Richmond district, and in an agreed upon area that EUC field support can provide this service. The region will be designated by codes/naming convention agreed upon with the VITA and documented within the SMM. The VIP Service Request will come to Iron Bow through the SMS into Cherwell. The Iron Bow Regional Manager will assign resources to execute the VIP support. Once the VIP support is completed, the ticket will be updated in Cherwell (integrated with the SMS).

VIP Support (Outside Richmond District - Rural): Service Requests received for VIP End Users outside of the Richmond District, but within a designated Rural area will be performed in accordance with the SLA's for VIP Support (Outside Richmond District - Rural). The Outside Richmond District (Rural) designation is defined as any geographical area outside the Richmond district, and in an agreed upon area that EUC field support can provide this service. The region will be designated by codes/naming convention agreed upon with the VITA and documented within the SMM. The VIP Service Request will come to Iron Bow through the SMS into Cherwell. The Iron Bow Regional Manager will assign resources to execute the VIP support. Once the VIP support is completed, the ticket will be updated in Cherwell (integrated with the SMS).

2. Provide expedited onsite IMAC and break/fix support for VIP Users.

The IMAC support as identified in Section 2.1.1 will be provided to any identified VIP under SLA's for VIP Support.

3. Upon VITA request, travel with VIP User to provide support.

Upon VITA request, members of Iron Bow will travel with VIP Users to provide support. While on travel, support will be provided on any type of IT issue needed.

4. Provide VIP User home support, which may require travel to personal residences, in accordance with the SMM and in accordance with VITA Rules.

As defined within the SMM and VITA Rules, Iron Bow will travel to personal residences to support VIP Users. In this instance, the Field Service Technician will stay until all issues are resolved and the VIP's systems are operational. Prior to executing this requirement, Iron Bow will discuss any liability issues with VITA and the Customer.

5. Configure and test computing Devices to ensure access to the VITA network through the VIP User's own network.

Field Service Technician will stay until all issues are resolved and the VIP's systems are operational. To ensure the VIP has connectivity prior to leaving the desk-side, Iron Bow will conduct a ping test, as well as navigating through the browser to the internet. Ping is a network administration utility or tool used to test connectivity on an IP network. To test network connectivity with ping:

Open the Command Prompt or Terminal. Every OS has a command line interface that allows running the Ping command, operating virtually identically on all systems as depicted in Table 4.

Table 4 Ping Commands Across Platforms

Windows	If using Windows, open the Command Prompt. Click the Start button and enter "cmd" into the Search field. Windows 8 Users will type "cmd" while on the Start screen. Press Enter to launch the Command Prompt.
Mac OS X	If using Mac OS X, open the Terminal. Open your Applications folder, and then open the Utilities folder. Select Terminal.
Linux	If using Linux, Open a Telnet/Terminal window. It is most often found in the Accessories folder in your Applications directory

6. Support, install, and configure non-standard Environments and technology in accordance with the SMM and VITA Rules.

Iron Bow will work with VITA and the VIP to understand what non-standard Environments exist and where they are located. Once the non-standard Environments are identified and the locations of the VIPs requiring such support, Iron Bow will ensure Field Service Technicians in that region have the training and tools they need to support, install and configure non-standard Environments, while maintaining a secure posture and compliance with SMM and VITA Rules.

2.3 Software Services

1. Provide a distribution service and system (the "Software Distribution System") for Software, including Operating System updates, Patches, new standard enterprise applications, Customer applications, etc.

Iron Bow will use SCCM as the Software distribution system. SCCM is a systems management Software product developed by Microsoft for managing large groups of computers running Windows NT, Windows Embedded, macOS (OS X), Linux iOS and Android mobile OS. SCCM provides remote control, Patch management, Software distribution, OS deployment, network access protection and Hardware and Software inventory. To supplement SCCM in servicing non-Windows Devices, Iron Bow will use [redacted] for 3rd party Patching. Iron Bow will provide the Software Services described in this contract for all supported Operating Systems and descriptions of processes for any specific Operating System are representative of the processes that Iron Bow will use to provide Software Services for all supported Operating Systems.

Iron Bow services include the packaging/install/update of End User Software (including printer drivers) on behalf of other Towers, in coordination with the MSI and VITA. Iron Bow will distribute Software for VITA. This will be part of the Services offered as part of Iron Bow's Software Services activities; no separate/additional charges will apply.

Iron Bow will continuously evaluate their suite of tools to ensure the level of service to VITA and Customers remain reliable and evolve with changing needs.

Iron Bow's Hardware and Software Services Team will consist of a team of 10 full time personnel as detailed below:

Responsibility	FTEs
Software Services Lead - MS SCCM Expert	1
SCCM Admin / Leads / Tier 3 Support (Sr.)	3
Image / Packaging Technicians / Tier 3 Support (Mid)	3
Imaging Technicians (Jr.)	3

2. Provide imaging, reimaging, Software packaging and deployment services (incl. Patching and Software updates) in accordance with the SMM and VITA Rules.

Iron Bow will use MDT, which is a unified collection of tools, processes, and guidance for automating desktop deployment. In addition to reducing deployment time and standardizing desktop images, MDT makes it easy for Iron Bow to manage security and ongoing configurations. MDT supports the deployment of Windows 10, as well as Windows 7, Windows 8, and Windows 8.1. It also includes support for zero-touch installation (ZTI) with SCCM. Regardless of the type of desktop image, Iron Bow's Hardware and Software Services Team will use MDT to build and maintain that image which fully automates the image building process. By automating that process, Iron Bow will get a consistent, stable result. MDT provides an interface that provides a consistent and repeatable image creation sequence every time removing the possibility of human error from the image-building process.

Iron Bow's Hardware and Software Services Team will deploy the image using SCCM, while using MDT to build and maintain the baseline image. Using SCCM provides Iron Bow with a great deal of flexibility and control on deployment and Patching. This includes a central location from which to review Patches and determine which ones are appropriate for the Customer and the Environment. SCCM allows Iron Bow to choose exactly which Devices to deploy each Patch to, and when the Patching takes place.

To create the actual Patch deployment, Iron Bow's Hardware and Software Services Team will start by reviewing the list of available Patches and create a group of Patches called a "Software update group." Next, Iron Bow will create groups of Devices called "collections." Iron Bow will use collections for tasks such as application management, deploying compliance settings, or installing Software updates. Iron Bow's Hardware and Software Services Team will also use collections to manage groups of Customer settings or use them, along with role-based administration, to specify the resources that an administrative User can access. Finally, Iron Bow will create a "deployment package" that deploys specific Software update groups to specified collections at a specified time.

See also Sections 2.3.1 through 2.3.3 for further details on Software Distribution, Client Image Engineering, and Patching and Updating. Iron Bow will use similar methodologies for other supported operating systems

3. Provide configuration and deployment services for VITA, VITA Customer specific, and COTS Software in accordance with the SMM and VITA Rules.

Configuration Management. Iron Bow's primary goal for desktop change and configuration management is to ensure that the computing resources that are necessary for Users to do their jobs are available when the Users

need them. The challenges to desktop management include centralizing control of many PCs, dealing with multiple computer Hardware and Software configurations, dealing with User accounts, and updating systems to address changing business needs. By using change and configuration management features — specifically Group Policy settings — Iron Bow will create and maintain the desktop for each User's work Environment. When managing the desktop, Iron Bow will work with the Customer to determine the type of User and computer configurations that are needed and the various settings that are required.

Through using Group Policy, Iron Bow will define and control how Software, network resources, and the OS functions for Users and computers. Within the Active Directory Environment, Group Policy will be applied to Users or computers based on the User or computer accounts that exist in sites, domains, or organizational units. Users and computers are the only types of Active Directory objects that receive policy. Through Group Policy, Iron Bow will control the behavior of the client computer and determine the characteristics of the client User Environment. Iron Bow will use Group Policy to manage items and Software available on the desktop. Iron Bow will interface with other STS's for any Group Policy actions in accordance with the SMM and VITA Rules.

Deployment Services. Iron Bow has divided the deployment scenario into different sub-scenarios:

New computer. This scenario occurs when there is a blank machine to deploy. The setup starts from a boot media, using CD, USB, ISO, or Pre-Boot Execution Environment (PXE). Iron Bow will also generate a full offline media that includes all the files needed for a deployment, allowing the Hardware and Software Services Team to deploy without having to connect to a central deployment share site or tool. The target will be a physical computer, a virtual machine, or a Virtual Hard Disk (VHD) running on a physical computer (boot from VHD). The deployment process for the new machine scenario is as follows: 1) Start the setup from boot media (CD, USB, ISO, or PXE); 2) Wipe the hard disk clean and create new volume(s); 3) Install the OS image; 4) Install other applications (as part of the task sequence). After taking these steps, the computer is ready for use.

Computer refresh. A refresh is sometimes called wipe-and-load. The process is normally initiated in the running OS. User data and settings are backed up and restored later as part of the deployment process. The deployment process for the wipe-and-load scenario is as follows: 1) Start the setup on a running OS; 2) Save the User state locally; 3) Wipe the hard disk clean (except for the folder containing the backup); 3) Install the OS image; 4) Install other applications; 5) Restore the User state. After taking these steps, the computer is ready for use.

Computer replace. A computer replace is similar to the computer refresh scenario. However, since the machine is being replaced, Iron Bow performs 2 main tasks: backup of the old client and bare-metal deployment of the new client. As with the refresh scenario, User data and settings are backed up and restored. The deployment process for the replace scenario is as follows: 1) Save the User state (data and settings) on the server through a backup job on the running OS and 2) Deploy the new computer as a bare-metal deployment.

4. Ensure the distribution/support process complies with VITA Rules and industry best practices (e.g., Microsoft CBB for Windows 10).

Iron Bow will provide for distribution and support which will be in compliance with VITA Rules. Iron Bow will take into consideration the Customer mission and the sensitivity and timing for deploying updates. As a Microsoft Gold Partner, Iron Bow keeps current with the latest developments and will provide distribution and support in concert with industry best practices. As an example, Windows 10 forced organizations to change the approach to deploying updates. Servicing channels are the first way to separate Users into deployment groups for feature and quality updates. With the introduction of servicing channels comes the concept of a deployment ring, which is simply a way to categorize the combination of a deployment group and a servicing channel to group Devices for successive waves of deployment.

To align with this new update delivery model, Windows 10 has 3 servicing channels, each of which provides different levels of flexibility for when these updates are delivered to client computers. As part of the alignment

with Windows 10 and Office 365 ProPlus, Microsoft adopted the following common terminology to make it as easy as possible to understand the servicing process: Semi-Annual Channel – Iron Bow will be referring to Current Branch (CB) as "Semi-Annual Channel (Targeted)", while Current Branch for Business (CBB) will simply be referred to as "Semi-Annual Channel" and Long-Term Servicing Channel - The Long-Term Servicing Branch (LTSB) will be referred to as Long-Term Servicing Channel (LTSC). Within this updated servicing model, the Semi-Annual Channel is twice-per-year, featuring update releases targeted around March and September, with 18-month servicing timelines for each release. The Semi-Annual Channel replaces the Current Branch (CB) and Current Branch for Business (CBB) concepts starting with Windows 10, version 1703, which released for broad deployment on July 27, 2017. Windows Update for Business deferral policies based on broad deployment readiness will be calculated from that date. With each Semi-Annual Channel release, Iron Bow will follow Microsoft recommendations to begin deployment right away to targeted Devices and ramp up to full deployment as VITA requires. This will enable the Customer to gain access to new features, experiences, and integrated security as soon as possible.

With the advent of the Microsoft Windows as a Service solution, Microsoft has revised and revamped the update and Patching approach to speed the delivery of new features and simplifying the process for staying current with Windows. Microsoft delivers Semi-Annual Feature Updates to minimize the impact from major changes 2 times per year, introducing less change while also reducing application compatibility impacts. Quality updates, containing security, reliability and bug fixes, are delivered once per month in a single cumulative monthly package that simplifies the process of updating machines, ensuring the full array of Patches are applied and makes updating offnet machines far easier and comprehensive.

Semi-Annual Feature Updates: Windows 10 uses an open and continual development process. Internally Microsoft releases daily engineering builds which are deployed and tested by thousands of engineers and testing professionals. These daily releases are then consolidated into periodic builds deployed into a broader internal Microsoft Internal Validation Audience. After 6 months, the builds are consolidated into a preview Semi-annual release that is made available to Windows Insiders. Leveraging the Windows Insider Preview Branch, Iron Bow will evaluate monthly Windows 10 builds for impact. After 6 months of releases, the Semi-Annual Release will be available for general usage and will be piloted to a select group of Semi-Annual Channel (Targeted) (Legacy CB) users. Once successfully tested and fully evaluated in a favorable fashion, both internally and by industry in general, typically after about 4 months, the feature update will be declared Semi-Annual Channel (Legacy CBB), indicating that it is ready for broad deployment.

For any release there are three phases: Evaluation; Pilot; and Broad Deployment. Each release will be serviced for 18 months from the initial date of release, meaning that at any given time there will be multiple releases in various stages of the deployment cycle at one time.

Monthly Quality Updates: In Windows 10, rather than receiving several updates each month and trying to figure out which apply to VITA, which ultimately causes platform fragmentation, Iron Bow will use one cumulative monthly update that supersedes the previous month’s update, containing both security and non-security fixes. This approach will make Patching simpler and ensure that End User Devices are more closely aligned with the testing done at Microsoft, reducing unexpected issues resulting from Patching.

VITA Deployment and Updating: Both the Semi-Annual Feature Updates and Monthly Quality Updates will be deployed to VITA by Iron Bow using SCCM for all on-network and internet connected Devices running Semi-Annual Channel (Targeted) (SAC-T), and Semi-Annual Channel (SAC) builds. Offnet machines running SAC and SAC-T builds will be handled by Iron Bow with a manual process, as detailed in Section 2.1.2.

An initial project will be undertaken by Iron Bow to get VITA and customer organizations standardized on the SAC or SAC-T releases of Windows 10. Once completed updates, both semi-annual and monthly, will be deployed by Iron Bow accordingly based on defined processes and procedures.

VITA Image Updates: The VITA Windows 10 SAC/SAC-T Image will be updated monthly by Iron Bow with the cumulative Monthly Quality Updates and then have the Semi-Annual Feature Updates integrated twice per year to coincide with Pilot and Broad Release deployment within VITA.

5. Provide other VITA approved distribution/support mechanisms that may be unique to Customer, group, or individual (e.g., Microsoft LTSB for Windows 10).

Iron Bow understands that with a broad User base, there will be customized distribution/support mechanisms unique to the Customer and Iron Bow will provide for this distribution and support. As an example, Windows 10 Enterprise LTSB is a separate LTSC version, as discussed above. It is designed to be used only for specialized Devices (which typically do not run Office). These specialized systems, such as those that control medical equipment, point-of-sale systems, and ATMs, often require a longer servicing option because of their purpose. These Devices typically perform a single important task and do not need feature updates as frequently as other Devices. The LTSC servicing model prevents Windows 10 Enterprise LTSB Devices from receiving the usual feature updates and provides only quality updates to ensure that Device security stays up to date. With this in mind, quality updates are still immediately available to Windows 10 Enterprise LTSB clients, but Customers can choose to defer them by using one of the servicing tools.

Microsoft never publishes feature updates through Windows Update on Devices that run Windows 10 Enterprise LTSB. Instead, it typically offers new LTSC releases every 2–3 years, which VITA will have the option to install as in-place upgrades or even skip releases over a 10-year life cycle. Iron Bow will work with Customers to determine the appropriate course of action pursuant to upgrades and follow such course of action for distribution and support.

For each unique customer, group, or individual use case, Iron Bow will analyze the requirements and recommend an approach to meeting their specific requirements. Iron Bow will recommend an appropriate service branch of Windows 10 and an appropriate Patching schedule based on each use case. These recommendations will consider both business and security requirements to offer the right balance for each scenario in compliance with VITA Rules. Iron Bow in conjunction with VITA, MSI and customer agencies, will determine the number of machines, their physical locations, the required Patching frequency, machine availability, and other factors. The Iron Bow project team will leverage various Windows, Security and other personnel as appropriate to define the approach to ensure compliance with all VITA Rules, MSI and SMM standards regarding security. Iron Bow will leverage the VITA approved Windows 10 OS wherever possible, and will only utilize Windows 10 Long-Term Servicing Channel (LTSB) in specific exceptions when approved by VITA in accordance with standards defined in SMM.

As part of the standardization on the VITA approved Windows 10 OS and the migration away from LTSB, Iron Bow in conjunction with VITA, MSI and Customers will identify all LTSB instances in use at VITA and all customer agencies. Iron Bow will organize these into two groups: 1) LTSB machines to be migrated to the VITA approved Windows 10 OS; 2) Candidate LTSB Exceptions to remain on LTSB (LTSC). Iron Bow will ensure all LTSB Exception candidates are successfully entered into the exception process as detailed in the SMM; any machines that fall out of/are note approved in this process will be added to the group of machines to be transitioned to the VITA approved Windows 10 OS.

Iron Bow understands that Microsoft will end support for Windows 7 on January 21, 2020 and therefore the Windows 7 remediation project must be completed prior to that date. To support VITA's ability to maintain a secure Environment, Iron Bow will develop a detailed plan to migrate the Windows 7 Devices. Iron Bow will

migrate the Windows 7 Devices according to the plan for such. The Windows 7 remediation project will be executed upon VITA's acceptance of the migration plan.

There are approximately 40,900 Windows 7 Devices. Some devices will be upgraded to Windows 10 as they are Refreshed in accordance with the Refresh Plan as described in **Section 8.1.3 of the Agreement**; remaining Windows 7 Devices will be migrated to Windows 10using one of two (2) approaches: Manual Touch estimated at 80% of the Devices and automated update estimated at 20% of the Devices.

Iron Bow will have a dedicated Windows 7 remediation team entirely focused on the timely completion of this work. That team will consist of a seasoned Project Manager (PM) who will be responsible for the overall execution and success of the project. Under the PM there will be two teams: 1) Image and Testing Team (ITT); and 2) Deployment Team (DT).

The ITT will consist of resources dedicated to developing and testing the Windows 10 (TPM 1.2) image for each applicable Customer and verifying with the Customer that their image and applications are working and resolving any issues that occur during testing. Iron Bow will do this by delivering the Customer image to 1 or more Devices for the Customer to confirm and accept the image, which will be done a fixed timeframe.

The DT will consist of several Lead Technicians and Deployment Technicians that will implement and execute the image deployment tasks. This team will be deployed in various ways, depending on the target site/Customer size, location and other factors, to deliver maximum efficiency in delivering the Windows 7 remediation. For a typical site, Iron Bow will leverage 1 Lead Technician with 4 or more Technicians under them (depending on size of site and/or time on site) to complete the tasks. These tasks include, but may not be limited to, confirming customer local data has been backed up, making an additional backup copy of the target profile's data, conducting the Windows reimaging, restoring the target profile data, and post migration support and assistance.

In addition to the standard manual installation, the DT will use automated upgrades in as many scenarios as possible. To accomplish this, the DT will coordinate with the larger Iron Bow team to deliver the image/migration tasks using the SCCM infrastructure. Iron Bow will deploy these upgrades remotely, where possible, but may also utilize an on-site server for deployment. For these automated upgrades, Iron Bow will perform tasks including, confirming customer local data has been backed up, making an additional backup copy of the target profile's data, conducting the Windows reimaging, restoring the target profile data, and post migration support and assistance.

High Level Windows 7 Remediation Steps

- **Image Development (beginning upon Effective Date)**
  - Define underlying base image leveraging TPM 1.2
  - Develop security and other settings to comply with STS requirements and VITA Rules
  - Receive approval from VITA to proceed with accepted base image
- **Agency Load Sets**
  - Identify all affected agency Customers
  - Rationalize application load sets
  - Validate Windows 10 compatibility
  - Validate TPM 1.2 settings don't compromise compatibility, VITA Rules and other security requirements for Agency applications
  - Work with Agencies to resolve/remediate any lingering Windows 10 compatibly issues with load sets.
  - Receive Agency signoff for image and load set(s)
- **Deployment and Project Planning**

  - Receive up-to-date inventory for all affected Devices to include:
    - All asset information
    - User information
    - Location information
    - Existing Image
    - Application Load set
  - Break down inventory by site, Customer, geographic location, or other dimensions to group machines as appropriate.
  - Identify automated deployment candidates
  - Develop Schedule
  - Optimize schedule based on site size, geographic location, availability windows, resources, etc.
  - Develop Resource Plan
  - Develop Communications Plan
  - Develop Risk Register
  - Develop other project artifacts
- **Schedule**
  - Image development and other planning activities will begin immediately upon Effective Date
  - Deployment will begin upon Commencement Date
  - Completion of all migrations by EOL Windows 7 date (Jan 21, 2020) – subsequently extended to December 31, 2020 subject to the remediation plan attached to this exhibit as Attachment A.
  - The above-referenced deadline of December 31, 2020, was missed and work continues for the completion of migrations. An updated remediation plan, attached to this Exhibit as Attachment B, shows a deadline extension to June 30, 2021 for the completion of all migrations.
  - Additional updates were necessary to the June 2021 submission referenced above. The parties (Iron Bow, MSI and VITA) have worked each device escalation pursuant to the terms identified in the approved Remediation Plan and escalation process (Attachment B). As of November 2021, EUS 3.10 will be Accepted with Conditions and all remaining Windows 7 devices will be tracked through various projects being managed by the MSI: Aging Architecture, PC Refresh and Windows 7 Hardware Aged Architecture. The assignment of these projects in KeyStone Edge tracks each device to project completion and successful migration and/or final disposition in which the agency chooses not to migrate the device and apply whitelisting.
- **Deployment**
  - Deploy according to plan
  - Test End User System to ensure they are operational
  - Provide over-the-shoulder support as needed for the End User

After Effective Date, Iron Bow will deliver a detailed project plan to VITA for acceptance that includes:

- Migration project plan which outlines key deliverables, dependencies, and Iron Bow and Agency/End User activities to include all project document artifacts
- Communications plan utilizing available medium (email, posters, newsletter, website, etc. as available/desired) to ensure all impacted Customers are informed of what is happening, when it is happening, and to set expectations for preparation and post migration activities
- Dedicated team to perform manual and automated deployments, focusing on minimizing disruption and reducing End User downtime

- Deployment plans/schedules and readiness meetings (kickoff, 45 days out, 14 weeks out, prior day, etc. as determined reasonable for each location) leading up to migration
- Migration and post migration reporting.

6. Provide an online application store for VITA and Customer approved Software in coordination with the MSI Portal.

Both SCCM and Cherwell offer the ability to deliver Software to users at their request based on numerous role-based, organization-based, or other controlling/limiting factors to determine who has access to what Software in the store. Iron Bow will leverage the Cherwell service catalog as the interface to enable User Self-Service and to meet the VITA app-store requirements. This will present the users with a consistent experience across all their IT service requests. SCCM will be used on the back end to deliver Software to users as ad-hoc (or scheduled) deployments.

The application catalog and portals will provide Users control over how and when Software is installed on their Devices. An advantage with SCCM is that it ensures that the Software that Users need in order to perform their work is available wherever they log on, not just on their primary Devices. Users of Windows-based computers can manage their Software deployment experience by using the client interface in Software Center. Software Center is automatically installed on client computers so that Users can manage their own Software. Users can connect to the Application Catalog where they can browse for, install, and request Software. Because the Application Catalog website is hosted in Internet Information Services (IIS), Users can also directly access the Application Catalog on a browser from the intranet or the Internet.

All Software offered in the catalog will be analyzed and tested to determine compatibility with Windows10. Software will then be packaged into a scripted/no-touch installation for the self-service portal. Service Requests will be logged through the MSI's Portal and will be routed through the appropriate approval workflows defined for each Software package relative to the end-user's organization. Once approved, Software will be delivered hands free and autonomously via SCCM/MDT to the endpoint. Any licensing data required will be recorded and synchronized in both SCCM and Cherwell to enable proper license management and reporting.

Each organization will ostensibly have its very own self-service Software store. Entitlement will be broken down per organization and role-based-access-control utilized to only show Users Software that they are entitled and approved to see. Additionally, each organization will have a test self-service portal to allow testing of new packages and other IT services as well as evaluation of new workflows/approval processes.

7. Provide VITA or Customer approved unique User or group configurations (e.g., web favorites, application features, desktop icons, etc.).

Iron Bow's primary goal of desktop change and configuration management is to ensure that the computing resources that are necessary for Users to do their jobs are available when the Users need them. By using change and configuration management features — specifically group policy settings — Iron Bow will create and maintain the desktop for each User's work Environment. When managing the desktop, Iron Bow will work with the Customer to determine the type of User and computer configurations that are needed and the various settings that are required.

Group policy is the primary tool Iron Bow will use for defining and controlling how Software, network resources, and the OS function for Users and computers. Within the Active Directory Environment, group policy will be applied to Users or computers on the basis of their User or computer accounts that exist in sites, domains, or organizational units. Through group policy, Iron Bow will control the behavior of the client computer and determine the characteristics of the client computer User Environment. Iron Bow will use group policy to

manage items and Software available on the desktop. Iron Bow will interface with other STS's for group policy actions in accordance with the SMM and VITA Rules.

8. Provide method(s) for End Users to use applications or Devices that require elevated privileges (e.g., power User, local administrator account) in accordance with the SMM and VITA Rules.

Iron Bow will use group policy security policies to restrict User access to files and folders and control User rights. See Section 2.3 #7 directly above.

9. Integrate Software distribution with MSI Service Request process to support self-provisioning.

Iron Bow will coordinate with the MSI to integrate Software distribution with support self-provisioning.

10. Perform User acceptance testing of all Software packages and images in accordance with the SMM and VITA Rules.

Once an image is defined and Software is packaged, Iron Bow will place it in a test Environment. The actual mechanics of testing may vary widely depending on the image/Software packages being tested and the size of the User population that the image is being provided. This testing may be simple, giving it to a subset of Users for beta testing or may involve the execution of a battery of detailed and elaborate test cases that validate functionality. Iron Bow will use a suitable approach toward User acceptance testing which will be dictated by criticality and availability requirements, available resources, and severity.

The initial phases of production will be considered an additional component of the testing process. With approval from the VITA, Iron Bow will perform rollouts in tiers, with the initial tiers targeting less critical systems. Based on the performance of these stages of the image/Software deployment process, the entire Environment will then be updated, and the testing process will be considered finished with the successful completion of final acceptance testing. All of Iron Bow's testing will be performed in accordance with SMM and VITA Rules and coordinated with the MSI, in addition to other STS as required.

11. Provide appropriate End User Devices to support Software testing.

Our relationships with the OEM's provide Iron Bow access to proof of concept and/or test Devices that will be utilized as needed to validate functional and technical requirements for new solutions, as well as Software testing. These Devices will be configured the same as the End User population is configured. All of Iron Bow's testing will be performed in accordance with SMM and VITA Rules and coordinated with the MSI, in addition to other STS as required.

12. Produce and regularly update detailed build documentation for Software packages and images in accordance with SMM and VITA Rules.

Software and image build documentation will be produced and regularly updated within MDT and SCCM in accordance with SMM and VITA Rules. Any narrative to support Software or image build process, such as Testing Plans, will be maintained in the MSI's Document Library. System build tools and guidelines are the primary enforcement means of ensuring compliance with requirements at installation time. As new Software/Patches/updates are approved and deployed, build images and scripts will be updated so that all newly built systems are appropriately Patched, and associated build documentation will be updated to reflect these changes. In addition to updates to build tools and documentation, operational procedures will exist to facilitate ongoing compliance of newly built systems. Any new Patches and updates that are approved and installed by operations will also be integrated by the engineering team into new builds, with the change management system providing both an appropriate audit trail and suitable procedural guidelines for the Implementation.

2.3.1 Software Distribution

1. Package, distribute, deploy and update Software through the Software Distribution System in accordance with the SMM and VITA Rules.

Iron Bow's software distribution system consists of 2 components for Windows: MDT and SCCM. These tools used together simplify the task of building, maintaining and deploying Windows images. Iron Bow will use MDT for building the baseline image and packaging and will then deploy these images using SCCM. For non-Windows Devices, Iron Bow will leverage [redacted] integrated with Iron Bow's SCCM infrastructure to manage non-windows (macOS, iOS, Android) endpoints.

Packaging. Iron Bow will use application packaging to efficiently manage the growing volumes of Software for VITA desktop systems. Application packaging involves the preparation of standard, structured Software installations targeted for automated deployment. Automated installations, or packages, will meet the installation requirements for each specific Environment. In addition, packages will be prepared for both commercial-off-the-shelf (COTS) Software and applications developed in-house. To enable this level of application management, Iron Bow will use MDT which is part of the desktop OS. This database-driven service resides on workstations and controls the installing, uninstalling, Patching, and repairing of Software.

To realize the benefits of application packaging, Iron Bow will provide the following activities: gathering requirements, using MDT, building a stable baseline image, managing conflicts, evaluating application suitability for packaging, establishing a centralized packaging process, creating a structure to group applications, and implementing a formal request process. Software packages created by Iron Bow will be included in the Definitive Software Library (DSL), subject to the procedures for the DSL within the SMM. Iron Bow's process for packaging includes the following:

- Use of Windows Installer. Microsoft's Windows Installer technology is designed to simplify the process of adding applications to the desktop and to minimize support costs by helping to eliminate errors associated with those installations. Iron Bow will provide an alternate tool as may be required for other OS.
- Application suitability for packaging. Although application packaging offers several benefits, certain applications will be deployed outside an automated Software distribution.
- Centralized packaging process. Although enterprises typically use numerous Windows-based applications, many enterprise IT organizations do not have a common organization or methodology for Software packaging and deployment. Selection of a MDT will facilitate this centralization.
- Structured application grouping. While some applications are used across an organization, others may be useful only to a certain business unit, geographic location, or group of specialized Users. By instituting a packaging process, Iron Bow will establish a structure for classifying and managing diverse Software used throughout the Commonwealth. Typical groupings include applications core to the business, those used primarily for departments or business units, and those deployed ad hoc to small groups of Users.
- Formal application request and approval process. Packaging technology allows Iron Bow to provide VITA and Customers with a formal process for requesting, approving, and distributing applications. A simple workflow process provides a way for Users to request a specific application and obtain approval. This process significantly aids in eliminating unnecessary application deployments while helping to ensure that End Users receive the appropriate, predefined versions of the requested applications.

Distribute, deploy and update Software. SCCM provides Iron Bow with a comprehensive solution for change and configuration management. SCCM will allow Iron Bow to perform tasks such as the following:

- Deploy OS, Software applications, and Software updates
- Monitor and remediate computers for compliance settings
- Monitor Hardware and Software inventory
- Remotely administer computers

See Section 2.3.3 Patching and Updating for detailed information about Iron Bow's methods for distributing, deploying, and updating Software.

2. Provide method (e.g., Software installation portal) by which End Users may self-install approved applications without requiring elevated privileges. Method must allow approved self-install applications to be provided at multiple levels (e.g., for any COV Device, for specific Customers, for specific groups).

SCCM has a built-in application web portal, where Users can browse from any supported Device to use or install Software or applications that have been made available to them. Iron Bow will use Group Policy to define the specific parameters.

3. Support all VITA-approved platforms.

Iron Bow will support all VITA approved platforms. SCCM runs on Windows, Windows Embedded, macOS (OS X), Linux , as well as iOS and Android mobile. The WIM format within MDT is completely Hardware-agnostic, capturing and/or deploying from any system. Iron Bow has included additional tools to supplement SCCM such as [redacted].

4. Provide all VITA-approved Software packages to Customers upon request (whether standard for the enterprise or unique to specific Customers, groups, or Users).

Iron Bow will provide all VITA-approved Software packages to Customers upon request, whether standard or unique to specific Customers, groups, or Users.

5. Provide capability to distribute Software (e.g., applications, drivers) to subsets of Devices (e.g., by Customer, groups, geographic locations).

SCCM allows establishment of deployment groups, which Iron Bow will use to define distribution of Software to subsets of Devices by Customer, groups, or location.

6. Support the installation of multiple approved concurrent versions of the Operating System or other Software on a single End User Device.

If the End User currently has one OS on a single partition spanning the entire disk, Iron Bow will resize that partition to make room for a separate partition for the other OS. Iron Bow will defragment the drive first (if necessary). There may be instances that Iron Bow will put each OS on a separate physical disk, but partitioning will be the preferred method. Iron Bow will check the system requirements for each OS and make sure each can get a partition at least that large. Iron Bow will also reserve some space for a data partition available to both OS. Different OS require partitions with different file systems. Iron bow will work with the End User to set the default for which OS to boot at start.

This can also be accomplished easily in a virtualized Environment as discussed in Sections 4.1, 4.2, and 4.3.

7. Distribute Software to all End User Devices, whether on or off the VITA network (including via Internet).

SCCM provides several methods to deploy Software. If Iron Bow has to deploy Software to a computer that is not connected to the network or to a computer that is connected by a low bandwidth connection, Iron Bow will use SCCM to create offline installation media that performs the installation or the User can pull the Software from the application catalog. Pre-staging content on a site server or distribution point, before distributing the content requires no transfer over the network. Alternatively, Iron Bow will pre-stage content files for applications and packages. Using the 'Create Pre-Staged Content File Wizard' Iron Bow will create a compressed, pre-staged content file that contains the files and associated metadata for the content. Then, Iron Bow will manually import the content at a site server or distribution point.

With SCCM, Iron Bow will leverage [redacted] which allows Iron Bow to manage SCCM clients while they are not connected to the Agency network, but have a standard Internet connection. [redacted] provides management of

internet-based clients using a combination of a Microsoft Azure cloud service, and a new site system role that communicates with that service. Internet-based clients use the cloud service to communicate with the on-premises Configuration Manager.

8. Implement an efficient methodology in which End User Devices are remotely inspected based on specific criteria to guarantee that a Patch, Software, or configuration update is applied.

SCCM provides many ways to monitor Software updates objects, processes, and compliance information. After deploying the Software updates in a Software update group or deploying an individual Software update, Iron Bow will monitor the deployment status. Iron Bow will also monitor content in the SCCM console to review the status for all package types in relation to the associated distribution points. This will include the content validation status for the content in the package, the status of content assigned to a specific distribution point group, the state of content assigned to a distribution point, and the status of optional features for each distribution point (content validation, PXE, and multicast).

State messages for Software updates provide information about the compliance of Software updates and about the evaluation and enforcement state of Software update deployments. Iron Bow will run Software update reports to display these state messages. There are more than 30 predefined Software update reports available. They are organized in several categories and will be used to report on specific information about Software updates and deployments. In addition to using the preconfigured reports, Iron Bow will also create custom Software update reports according to the needs of the Customer.

9. Initiate timely distribution to End User Devices that were not accessible during initial distribution.

Prior to re-initiating distribution, Iron Bow will first determine the client status. After Software has been deployed Iron Bow will run tests to check for status; view an update on deployment and compliance percentage; check which machines successfully received the Software; and determine which are in the process, which failed, and which have an unknown status. 'Unknown' status simply means that the machine has not yet checked in with SCCM, so SCCM does not know status in the Patching process.

The client health evaluation (Patching) also involves checking the health of the client and the clients are marked as either Passed, Failed or Unknown, along with the Active/inactive client health status. This results in the following possible client health states: Active/Pass; Active/Fail; Active/Unknown; Inactive/Pass; Inactive/Fail; and Inactive/Unknown. The client health evaluation will be done by the client by running the ccmeval.exe tool on schedule (via schedule task) once per week. The [redacted] schedule task creation are part of the SCCM client installation. The results of the client health evaluation will be found in the SQL View. The 'Fail' state generally indicates the following possible problems with the client: client prerequisites; MS agent host service status; client WMI provider; SCCM remote control service status; client installation; BITS issue; and Windows Update service startup type. Logs will be used to determining the underlying issue so that Iron Bow is able to correct the client issue prior to re-initiating deployment. The 'Unknown' state means that the client health state evaluation has not run on the PC or may have not reported to the SCCM server. This usually occurs when the PC is imaged (in a depot scenario) and stored in shelf for distribution later. After the issue is identified, Iron Bow will redeploy the Software/Patch.

10. Schedule Software distributions to minimize User disruption, and without (or minimizing) User assistance and interaction.

Iron Bow will ensure that scheduling guidelines and plans exist for both the Software distribution and Patch management program. First, a Routine Patching Plan will be developed by Iron Bow that guides the normal application of Patches and updates to systems. This plan does not specifically target security or other critical updates. Instead, this plan is meant to facilitate the application of standard Patch releases and updates. This plan can be time or event based; for example, the schedule can mandate that system updates occur quarterly,

or a cycle may be driven by the release of service packs or maintenance releases. In either instance, modifications and customizations will be made based on availability requirements, system criticality, and available resources. For prioritization, Iron Bow will use the OEM recommendations to develop Patch schedules or will prioritize as required by VITA.

Secondly, Iron Bow will collaborate with the MSS to develop a Security Patch Plan, subject to VITA acceptance, that will describe the methodologies required to deal with critical security and functionality Patches and updates. This plan will assist Iron Bow, the MSS, and VITA in prioritizing and scheduling updates that must be deployed immediately. The MSS and Iron Bow will consider a number of factors to determine Patch priority and scheduling urgency. Responses to information security and vendor-reported criticality (e.g. high, medium, low) will be key inputs for calculating a Patch's significance and priority, as is the existence of a known exploit or other malicious code that uses the vulnerability being Patched as an attack vector. Other factors that will be taken into account by Iron Bow when scheduling and prioritizing Patches are system criticality (e.g. the relative importance of the applications and data the system supports to the overall business) and system exposure (e.g. DMZ systems vs. internal file servers vs. client workstations).

11. Offer choices, where approved by VITA and in accordance with the SMM, for Customers or Users to select specific distribution time windows or to pull approved updates directly.

Iron Bow will use SCCM to set specific distribution windows and/or to pull approved updates from the application catalog. Iron Bow will work with VITA to enable these options for those Patches which are not deemed critical. Iron Bow will monitor Patch status closely to ensure compliance.

Pre-staging content on a site server or distribution point before distributing the content requires no transfer over the network. Iron Bow will pre-stage content files for applications and packages. Using the 'Create Pre-Staged Content File Wizard,' Iron Bow will create a compressed, pre-staged content file that contains the files and associated metadata for the content. Then, Iron Bow will manually import the content at a site server or distribution point.

12. Link Software distributions and End User Device inventories to verify the success of deployments and to provide the ability to track configurations and validate inventory.

SCCM is a Microsoft SQL Server (MSSQL) database that is used to verify success of deployments, as well as asset discovery. SCCM integrates with Cherwell so that inventory data (i.e., desktops, laptops, installed programs/Software, and installed services) is shared with and used within the Cherwell Service Management Configuration Management Database (CMDB) as Configuration Item records. Cherwell Asset Management automatically discovers all the Hardware and Software installed on Windows, Linux, and MAC OS, laptops, and servers, and reconciles discovered applications and Devices with purchasing details - what's installed, who's using it, and whether it's properly licensed. Cherwell Service/Asset Management will enable Iron Bow to leverage existing SCCM implementation and transform its raw inventory data into reliable, license-centric reports, while also tracking the success of Software deployments.

13. Provide automatic detection and remediation to bring End User Devices into compliance if any tracked security Patches are missing.

Deploying clients across the Customer base takes time and some installations are not successful the first time. Iron Bow will use the SCCM console to monitor client deployments within a collection (group) by reporting client deployment status in real time. In the SCCM monitoring workspace there is a node for distribution status. This node contains three sub-nodes that offer 3 different ways Iron Bow can view distributions: content status, distribution point group status, and distribution point configuration status; Iron Bow will utilize all different views. See also Section 2.3.1 #9 above.

Content Status provides a view of all the content objects that have been created in the SCCM hierarchy. From the content status node, Iron Bow can see the information about each package such as name, type (boot image, application, driver package, etc.), number of distribution points targeted, and compliance rate. This gives Iron Bow a view into content readiness on the per object level. In the detailed status, Iron Bow separates each state into its own tab to view (success, in progress failed and unknown). For each tab Iron Bow can see all the available statuses for the state and the affected assets for each status. When a status is selected, Iron Bow can see all the assets affected, more detailed message information and the last time of the status.

Distribution Point Group Status provides a view of distribution status to all the distribution point groups in the SCCM hierarchy. From the distribution point group status node, Iron Bow can see the distribution point group name, description, member count, and number of content objects assigned to the group for distribution. Iron Bow can also see the overall group state and compliance rate of the content distributed to the group. Just like the content status node, Iron Bow has the ability to "view status" for more detailed information. When Iron Bow views status, the same tab view and status summarization is available as the content status node. One difference to this view is when Iron Bow selects a summarization there will be an entry for per distribution point per package. This way if packages are failing for different reasons Iron Bow can provide the detailed message. Iron Bow can then select a column header in the asset details and group the by assets or package name.

Distribution Point Configuration Status provides a view of the configuration of a distribution point. This view is slightly different from the other 2 nodes. In this view Iron Bow is looking at the status of the content in addition to optional components such as PXE and Multicast. Since this node is intended for more than just content status, Iron Bow does not have the standard view status the other two nodes have. From this node Iron Bow have an easy access tab to view all the status messages associated with this distribution point.

Content validation checks the status of content that has already been distributed on a distribution point. From the content property page of a distribution point or distribution point group, Iron Bow will select a package and click the validate button. When this action is initiated the site server sends a command to the distribution point provider to validate the hash of the package on the distribution point. Once the action is completed the distribution point provider reports back to the site server and updates the compliance status in the distribution status node. This means if the hash comes back as not compliant on the distribution point Iron Bow will see the status node change its compliance to reflect the invalid package. While Iron Bow does not automatically remediate the invalid content on the distribution point, an administrator will redistribute the content to correct the error within 24 hours. Iron Bow will also perform this same type of action from the content locations tab on a package.

Another way Iron Bow will be able to validate content is on a schedule per distribution point. When the schedule runs, it performs a hash of each package individually on the distribution point and reports the status to the site server. For each package hash that is determined as invalid, the compliance status will be reflected in the distribution status node from the monitoring workspace. Iron Bow will establish the schedule using 1 of 2 methods depending on the Customer. The first is during distribution point role setup. The second is from the property page of the distribution point. On the property page there is a new tab called content validation. On this tab Iron Bow can set up a schedule for the task to occur. A task can be set to run at customizable frequencies. It also offers the ability to set the process priority. This will allow Iron Bow to regulate the performance impact on the server. The validation task is run locally by the distribution point provider and uses the Windows task scheduler.

The SCCM console also provides a chart of failed client deployments over a specified period of time which will allow Iron Bow to determine if actions to troubleshoot deployments are improving the deployment success rate over time. To expedite remediation, Iron Bow staff will use a standard checklist to identify and resolve the issue.

14. Provide to MSI the Software distribution data and statistics (including target counts and success results).

SCCM offers a variety of reports that Iron Bow will customize for this project. Iron Bow will work with the MSI and VITA to design reports to include all of the desired information, as well as the regularity of the reporting.

15. Resolve all instances where the Software distribution failed in accordance with the SMM.

Using the data collected in 2.3.1 #13 above, Iron Bow will work to resolve all instances where Software distribution failed in accordance with the SMM.

16. Continually review and improve the percentage of End User Devices that can be reached and updated with the electronic Software Distribution System.

Iron Bow will provide for regular audits and assessments that will help Iron Bow to gauge the success and extent of Iron Bow's Software distribution efforts. There are 2 critical success factors to audit and assessment: accurate and effective asset and host management. SCCM will be integrated with Iron Bow's Cherwell Asset Management System allowing Iron Bow to accurately track deployed Hardware and Software throughout the enterprise, including remote Users and office locations. Host management Software will allow Iron Bow administrators to generate reports (e.g. all End Users without a given hot fix, all versions of particular applications) that are used to drive the effort toward consistent installation of Software, Patches and updates across the organization.

System discovery and auditing are also components of the audit and assessment process. Asset and host management systems will help Iron Bow to administer and report on the Devices, however there are likely a number of Devices that have not been included in the asset and host management systems. Iron Bow will use system discovery tools to uncover these systems and assist in bringing them under formal system management and Patch compliance. The goal is to discover unknown systems within the Environment and assess their compliance with organization update and configuration guidelines. The SCCM console also provides a chart of failed client deployments over a specified period of time which will allow Iron Bow to determine if actions to troubleshoot deployments are improving the deployment success rate over time. To expedite remediation, Iron Bow staff will use a standard checklist to identify and resolve the issue.

17. Provide alternative Software distribution processes to support different User Environments (e.g., VITA LAN and WAN, home offices, Users working remotely), which may include via USB or CD.

See Section 2.3.1 #7 above and #18 and #19 directly below.

18. Provide automated distributions so that the Software deployment at low-bandwidth end points does not require User input.

Iron Bow's Hardware and Software Services Team will automatically deploy Software updates where practicable by using an automatic deployment rule (ADR). Typically, Iron Bow will use ADRs to deploy monthly Software updates and for managing definition updates.

19. Throttle distribution based on bandwidth limitations and/or quotas to minimize impact to Users.

To manage network bandwidth that is used for the content management process of SCCM, Iron Bow will use built-in controls for scheduling and throttling. Scheduling and throttling controls will be used for site-to-site communication, and for communication between a site server and a remote distribution point. If network bandwidth is limited even after setting up the scheduling and throttling controls, Iron Bow will pre-stage the content on the distribution point.

In SCCM, Iron Bow will set up a schedule and specify throttling settings on remote distribution points that determine when and how content distribution is performed. Each remote distribution point can have different configurations that help address network bandwidth limitations from the site server to the remote distribution point. The controls for scheduling and throttling to the remote distribution point are similar to the settings for a standard sender address. In this case, the settings are used by a new component, called package transfer

manager, which distributes content from a site server, as a primary site or secondary site, to a distribution point that is installed on a site system. The throttling settings are specified on the rate limits tab, and the scheduling settings are specified on the schedule tab, for a distribution point that is not on a site server. The time settings are based on the time zone from the sending site, not the distribution point.

Pre-staging content on a site server or distribution point before distributing the content requires no transfer over the network. Iron Bow will pre-stage content files for applications and packages. Using the 'Create Pre-Staged Content File Wizard,' Iron Bow will create a compressed, pre-staged content file that contains the files and associated metadata for the content. Then, Iron Bow will manually import the content at a site server or distribution point.

20. Ensure that no changes (e.g., Software Patches, driver installs) are applied to the Managed Environment without following the change management process in accordance with the SMM.

All system modifications, Patches, drivers, and updates will be performed and tracked by Iron Bow in accordance with the Change Management process in the SMM. SCCM provides for centralized management of Software distribution which provides Iron Bow with the ability to track systems, plan changes, and report on the results. The Change Management process used by Iron Bow will include testing the Patches and drivers prior to introduction to the Environment in accordance with Iron Bow's comprehensive testing process. The testing processes include test planning; test design; test execution; test validation and release; and test documentation. Iron Bow will perform testing, validation, and releases in accordance with the Release and Deployment Plan on Devices, OS, applications, and any changes made thereto.

21. Provide an option for visual status dialog to the User, conveying customized deployment action or information.

Within the user experience page in SCCM, Iron Bow has the ability to configure the following settings:

- User notifications: Specify whether to display notification of the Software updates in software center on the client computer at the configured Software available time and whether to display User notifications on the client computers.
- Deadline behavior: Specify the behavior that is to occur when the deadline is reached for the Software update deployment. Specify whether to install the Software updates in the deployment. Also specify whether to perform a system restart after Software update installation regardless of a configured maintenance window.
- Device restart behavior: Specify whether to suppress a system restart on workstations after Software updates are installed and a system restart is required to complete the installation.

22. Provide an option to restart or shutdown a system after a Software deployment has successfully completed, after providing a visual status dialog.

Iron Bow will configure settings to drive Device restart behavior. Device restart behavior specifies whether to suppress a system restart on workstations after Software updates are installed and a system restart is required to complete the installation. Iron Bow does not want the computers that are installing the Software updates to restart by default. However, doing so leaves computers in an insecure state, whereas allowing a forced restart helps to ensure immediate completion of the Software update installation. SCCM provides Iron Bow the ability to determine this behavior.

23. Provide a method that allows Users to delay deployments within a defined deployment timeframe.

Within ADR, Iron Bow will determine the rule for schedule evaluation, software available, and installation deadline. Installation deadline allows Iron Bow to specify the installation deadline for the Software updates in the deployment in 3 ways:

- As soon as possible: Select this setting to automatically install the Software updates in the deployment as soon as possible.
- Specific time: Select this setting to automatically install the Software updates in the deployment at a specific date and time. SCCM determines the deadline to install Software updates by adding the configured specific time interval to the Software available time.
- Deferred reboot: This allows the end user to delay the reboot up to a pre-defined amount of time.

The actual installation deadline time is the displayed deadline time plus a random amount of time up to 2 hours, which gives the Users some flexibility.

24. Document each deployment in accordance with the SMM and VITA Rules.

Iron Bow will produce documentation before and regularly update such documentation after each deployment in accordance with SMM and VITA Rules. As new Software/Patches/updates are approved and deployed build images and scripts will be updated so that all newly built systems are appropriately Patched, and associated build documentation will be updated to reflect these changes. In addition to updates to build tools and documentation, operational procedures will be revised based on the outcome of the deployment. Iron Bow will institute a lessons learned process to funnel such changes or other recommendations back to the build and engineering stage of the lifecycle. Any new Patches and updates that are approved and installed will also be integrated by the engineering team into new builds, with the Change Management System providing both an appropriate audit trail and suitable procedural guidelines for this implementation.

25. For each Software package, gather or develop appropriate documentation. This will include at a minimum:

25.1 Document how to install, configure, and execute the application prior to packaging.

25.2 Document what updates or Patches of a Software application to installation are needed for installs.

25.3 Document how to do basic testing of the application to determine if the package works.

25.4 Identify VITA, Customer, or Third Party subject matter expert for additional configuration and troubleshooting.

25.5 Document and communicate what End User will need to know or do before, during, and after package installation (e.g., do not use computer during install, reboot after).

Software and image build documentation will be produced and regularly updated by Iron Bow within MDT and SCCM in accordance with SMM and VITA Rules. Any narrative to support Software or image build process, such as testing plans, will be maintained in the MSI's Document Library.

Iron Bow will develop detailed documentation on how to install, configure and execute the application prior to packaging. For each Software package, Iron Bow will document what updates or Patches are to be install. As these modifications are approved and deployed, build images and scripts are updated so that all newly built systems are appropriately Patched, and associated build documentation is updated to reflect the changes. Iron Bow will develop a test plan to stipulate test Environment and test cases, with detailed steps for various types of testing and validation required. Testing includes how applications can be packaged, ability to coexist with other products in the package, as well as compatibility with the approved Hardware and OS. Iron Bow will document the results and make entries/updates to the CMDB and CI to reflect changes.

Iron Bow will document if there was a need for any third party experts, Customers, or VITA personnel for troubleshooting. Additionally, Iron Bow will document and communicate with the End Users how they should prepare for the deployment. The size and impact of the installation will dictate the level and medium of the information communicated. If the impact of the installation is significant, training or how to guides will be provided by Iron Bow. For other smaller deployments, a system notice may be all that is needed and will be

provided by Iron Bow. Special instructions will be provided, in addition to the numbers/emails to contact Iron Bow's support team if help is needed.

2.3.2 Client Image Engineering

Iron Bow's client image engineering services will include, but may not be limited to the following:

1. Estimate storage requirements for deployment on SCCM / distribution servers and storage requirements for backing up user state data (or backup locally)
2. Plan for application deployment
   a. Create app portfolio
   b. Identify dependencies
   c. Determine whether to deploy applications with the operating system image or afterwards
   d. Determine appropriate method for app execution
   e. Identify applications that require restarts and plan accordingly
3. Define Operating Systems components and settings
4. Choose deployment method – SCCM/deployment share or media based
5. Evaluate Network requirements
6. Choose image approach (thick, thin, hybrid)
7. Determine deployment scenario – new user, refresh, replace
8. Plan drive encryption
9. Evaluate target computer readiness
10. Verify target computer readiness
11. Verify target computer has adequate resources
12. Evaluate 64/32-bit differences/restrictions
13. Evaluate Device security settings and coordinate with security group to ensure compliance
14. Ensure deployment monitoring is configured

1. Develop, test, and update a set of standard VITA-approved images for use on End User Devices in accordance with the SMM and VITA Rules.

The baseline configuration provided by Iron Bow will define the lowest common denominator of what is needed for all the systems in the COVA Environment and will include the software listed in the Supported and Managed Software List, which VITA will provide to Iron Bow upon the contract Effective Date. To stay current and valid, Iron Bow will regularly evaluate and refresh the baseline standard image, adding new Software, revisions, and updates as necessary and as required by VITA. Such updates will be included in the Supported and Managed Software List. This includes addressing any emerging security technologies or threats that may require across-the-board revisions to the security settings. Iron Bow recommends that this reevaluation of the baseline configuration be performed on a monthly or quarterly basis and Iron Bow will conduct this reevaluation based on the VITA recommended procedures. The baseline includes the image as well as the set of specifications that define that image, the scripts that build that image, and the upgrade paths that bring existing systems into line with the current image. As Iron Bow issues a new baseline image, an upgrade pack is also issued so that Customers with previous versions can bring their baseline up to the new, current standard. The process includes the steps in the following sections.

Develop an Apps List: Iron Bow will first obtain or create/revise a list of applications that everyone in the VITA-supported enterprise requires. This will be the baseline and will only include the applications that every single computer absolutely needs. Iron Bow will not include applications that only a subset of Users will need. Iron Bow will use the Software delivery system to augment the baseline image with those applications later on. Part of this step includes specifying the version, publisher, and any updates that are required for a basic installation and

crucial add-ins and plug-ins are also included in this process. A typical baseline set of applications includes Microsoft Office, antivirus software, plug-ins for Internet Explorer, and any necessary internal line-of-business applications.

Security Settings: Iron Bow will perform a security threat analysis and propose settings in a checklist format. Settings should safeguard the organization against intrusion yet still allow Users to be productive. [redacted] provides a good starting point. These documents are critical to use as benchmarks since they include a lot of information on the known effects of certain restrictive settings. This information will allow Iron Bow make recommendations to VITA for forming their security configuration.

Building the Image: Once decisions are made by VTIA regarding applications and security, Iron Bow will implement these decisions by creating a single baseline system configuration. This configuration is then packaged into an image with MDT. MDT automates the build process that produces the final image and runs the system preparation tool just prior to capturing the image.

Quality Assurance and Testing: Once the image is complete, quality assurance testing, operational testing, and pilot usage will be conducted by Iron Bow prior to being submitted for approval and delivery to production.

2. Ensure that all End User Devices are imaged via a VITA-approved imaging process prior to being connected to VITA's network Environment in accordance with the SMM and VITA Rules.

Iron Bow will image all End User Devices with the approved baseline image. Iron Bow's Hardware and Software Services Team will load the baseline image at Iron Bow's lab prior to being connected to VITA's network. The agency load set, asset tag and logging will also be completed at the imaging lab. Iron Bow will not connect devices without VITA approved images to the COV network. See Section 2.3.2, Client Image Engineering, #5 below for an outline of the process.

3. Gather imaging, packaging and testing requirements from VITA, the MSI, other Tower Suppliers, Third Party Vendors, and Customers as applicable.

The Iron Bow staff responsible for image engineering will perform data gathering to collect the needed details about each application, imaging, packaging, and testing requirements. Our engineers are experienced in creating MDT packages and will be responsible for gathering the technical data to do so. Data will be collected via a questionnaire or a series of short interviews of VITA, incumbent staff, the MSI, or other Tower Suppliers. While some applications are used across an organization, others may be useful only to a certain business unit, geographic location, or group of specialized Users. By instituting a data gathering process, Iron Bow will establish a structure for classifying and managing diverse Software used throughout the enterprise. Typical groupings include applications core to the business, those used primarily for departments or agencies, and those deployed ad hoc to small groups of Users. Testing will be based on End User requirements for performance and function. Research will provide Iron Bow the data needed to define, package and test the image for maximum applicability and capability.

4. Engineer, package, test, and house images and image profiles in accordance with the SMM and VITA Rules

Iron Bow engineers will not begin packaging until the baseline image has been defined and stabilized. Attempts to build and test packages on early versions of the baseline image typically lead to significant reworking of the packages on the final baseline image.

Iron Bow will leverage relationships with Microsoft as a Gold Partner for Devices and Deployment. Iron Bow's EUC staff will communicate and work with corporate certified professionals when needed. Iron Bow will recommend changes to the enterprise baseline development structure based upon enterprise growth and evolution of technologies. Iron Bow will continue to leverage MDT in the image build process. The following

steps underpin the methodology Iron Bow will use: build and capture OS reference machine; create the image and distribute to distribution points; create and configure the appropriate deployment task sequence; deploy task sequence; and create packages for OS deployments. Iron Bow will develop, design, engineer, test, and document processes for provisioning and subsequent maintenance of desktop Software in support of the baseline image. Iron Bow will use the baseline image in all image builds for the various Hardware platforms and install all approved 3rd party Software with the settings stated in the security policy for those applications.

Iron Bow will provide application packaging that involves the preparation of standard, structured Software installations targeted for automated deployment. Automated installations, or packages, will meet the installation requirements for a specific Environment. Requirements include, but are not limited to: VITA standards for Software usage and desktop design, regional issues, and Software-related support issues. In addition, packages will be prepared for both commercial-off-the-shelf (COTS) Software and applications developed in-house.

To realize the benefits of application packaging, Iron Bow will perform the following activities: gathering requirements, using MDT, building a stable core image, managing conflicts, evaluating application suitability for packaging, establishing a centralized packaging process, creating a structure to group applications, and implementing a formal request process.

Use of Windows Installer. Iron Bow will use Microsoft's Windows Installer technology which is designed to simplify the process of adding applications to the desktop and to minimize support costs by helping to eliminate errors associated with those installations. Iron Bow will provide an alternate tool as may be required for other OS.

Application suitability for packaging. Although application packaging offers several benefits, certain applications will be deployed outside an automated Software distribution.

Centralized packaging process. Iron Bow will use MDT as the centralized methodology for Software packaging and deployment.

Structured application grouping. While some applications are used across an organization, others may be useful only to a certain business unit, geographic location, or group of specialized Users. By instituting a packaging process, Iron Bow will establish a structure for classifying and managing diverse Software used throughout the Commonwealth. Typical groupings include applications core to the business, those used primarily for departments or business units, and those deployed ad hoc to small groups of Users.

Formal application request and approval process. Iron Bow's centralized packaging process also provides for a formal process for requesting, approving, and distributing applications. A simple workflow process provides a way for Users to request a specific application and obtain approval. This process helps to eliminate unnecessary application deployments while helping to ensure that End Users receive the appropriate, predefined versions of the requested applications.

5. Provide method(s) for deploying images to Devices that are online or offline.

SCCM provides several methods Iron Bow's Hardware and Software Services Team will use to deploy an OS. Regardless of the deployment method used there are several standard actions that Iron Bow will take. These actions include the following and a similar methodology will be used for both Windows and all other OS:

1. Using MDT, import source files to management computer to include Windows OS files, OS language packs and Patches, Device drivers, and applications
2. Create task sequence and boot image for reference computer
3. Update deployment share with source files, boot image and task sequence
4. Transfer source files, boot image and task sequence from deployment share to the reference computer

5. Run [redacted] on the reference computer and capture image
6. Send captured image back to the management computer
7. Create task sequence and boot image for target computer(s) using captured reference image as source
8. Update deployment share with boot image, source files and task sequence
9. Transfer source files, boot image and task sequence from the deployment share to the target computer(s)
10. Run [redacted] on the target computers via SCCM or physical media

Methods Used to Deploy Operating Systems

There are several methods that Iron Bow will use to deploy OS to SCCM client computers, which are as follows:

- **PXE initiated deployments**: PXE-initiated deployments let client computers request a deployment over the network. In this method of deployment, the OS image and a Windows PE boot image are sent to a distribution point that is configured to accept PXE boot requests.
- **Multicast deployments**: Multicast deployments conserve network bandwidth by concurrently sending data to multiple clients instead of sending a copy of the data to each client over a separate connection. In this method of deployment, the OS image is sent to a distribution point. This in turn deploys the image when client computers request the deployment.
- **Bootable Media Deployments**: Bootable media deployments allow the OS to deploy when the destination computer starts. When the destination computer starts, it retrieves the task sequence, the OS image, and any other required content from the network. Because that content is not included on the media, Iron Bow will update the content without having to re-create the media.
- **Stand-alone Media Deployments**: Stand-alone media deployments allows the OS to deploy in the following conditions:
  - In Environments where it is not practical to copy an OS image or other large packages over the network
  - In Environments without network connectivity or low bandwidth network connectivity
- **Pre-staged Media deployments**: Pre-staged media deployments are used to deploy an OS to a computer that is not fully provisioned. The pre-staged media is a Windows Imaging Format (WIM) file that will be installed on a bare-metal computer by the manufacturer or at an enterprise staging center that is not connected to the SCCM Environment.

Later, when the computer starts in the SCCM Environment, the computer starts by using the boot image provided by the media, and then connects to the site management point for available task sequences that complete the download process. This method of deployment will reduce network traffic because the boot image and OS image are already on the destination computer. Iron Bow will specify applications, packages, and driver packages to include in the pre-staged media.

When Iron Bow has to deploy an OS to a computer that is not connected to the network or to a computer that is connected by a low bandwidth connection, SCCM will be used to create offline installation media that perform the installation.

6. Provide the ability to customize the Image process to meet the requirements of VITA or Customers.

Iron Bow will use MDT to build and maintain and provide both normal and customized images. Iron Bow will be able to fully automate the image building process with MDT, and by automating that process, get a consistent, stable result. MDT provides an interface that provides a consistent and repeatable image creation sequence every time. This removes the possibility of human error from the image-building process. A physical computer is no longer needed for building images. Iron Bow will use [redacted] to build Windows 10 images.

While the baseline image is built with MDT, SCCM (or Iron Bow's other tools for non-Windows Devices) will be used to distribute the image to End Users.

7. Provide the ability to name End User Devices in accordance with the SMM and VITA Rules.

Iron Bow will provide the ability to name End User Devices in accordance with the SMM and VITA Rules. User Device affinity in SCCM is a method of associating a User with one or more specified Devices. User Device affinity eliminates the need to know the names of a User's Devices in order to deploy an application to that User. Instead of deploying the application to all of the User's Devices, the application is deployed to the User. Then, User Device affinity automatically ensures that the application installs on all Devices that are associated with that User. Iron Bow will define primary Devices. These are typically the Devices that Users use on a daily basis to perform their work. When Iron Bow creates an affinity between a User and a Device, more Software deployment options are available. For example, if a User requires Microsoft Office Visio, Iron Bow will install it on the User's primary Device by using a Windows Installer deployment. However, on a Device that is not a primary Device, Iron Bow might deploy Microsoft Office Visio as a virtual application. Iron Bow will also use User Device affinity to pre-deploy Software on a User's Device when the User is not logged in. Then, when the User logs on, the application is already installed and ready to run.

8. Allow for multiple re-imaging per year as directed by VITA or Customer in accordance with the SMM and VITA Rules.

Iron Bow will provide for multiple re-imagings per year as directed by VITA or the Customer in accordance with SMM and VITA Rules. To re-image, Iron Bow has 2 options to use based on the Customer, number of Devices, timeframe, and complexity. Iron Bow will use similar methodologies for other supported operating systems:

- Upgrade Windows to the latest version: This scenario upgrades the OS on computers that currently run Windows 7, Windows 8, Windows 8.1, or Windows 10. The upgrade process retains the applications, settings, and User data on the computer. There are no external dependencies, such as the Windows ADK and this process is faster and more resilient than traditional OS deployments.
- Refresh an existing computer with a new version of Windows: This scenario partitions and formats (wipes) an existing computer and installs a new OS on the computer. Settings and User data are migrated after the OS is installed.

2.3.3 Patching and Updating

The main objective of Iron Bow's Patch management program will be to create a consistently configured Environment that is secure against known vulnerabilities in OS and application Software. Iron Bow will review a number of different pieces of information to design and implement a reliable Patch management program for VITA. For example, Iron Bow will be using SCCM for Windows-based systems, supplemented by [redacted] for macOS (OS X), Windows phone, iOS, Android Mobile OS.

As the End User Environment evolves and more macOS, iOS, and Android Mobile OS become a larger part of the supported Devices, Iron Bow will continue to evaluate and assess tools for Patching. Iron Bow will follow the high-level process illustrated below in Figure 2 as a means to assess the current Patch management efforts and make recommendations, accordingly.

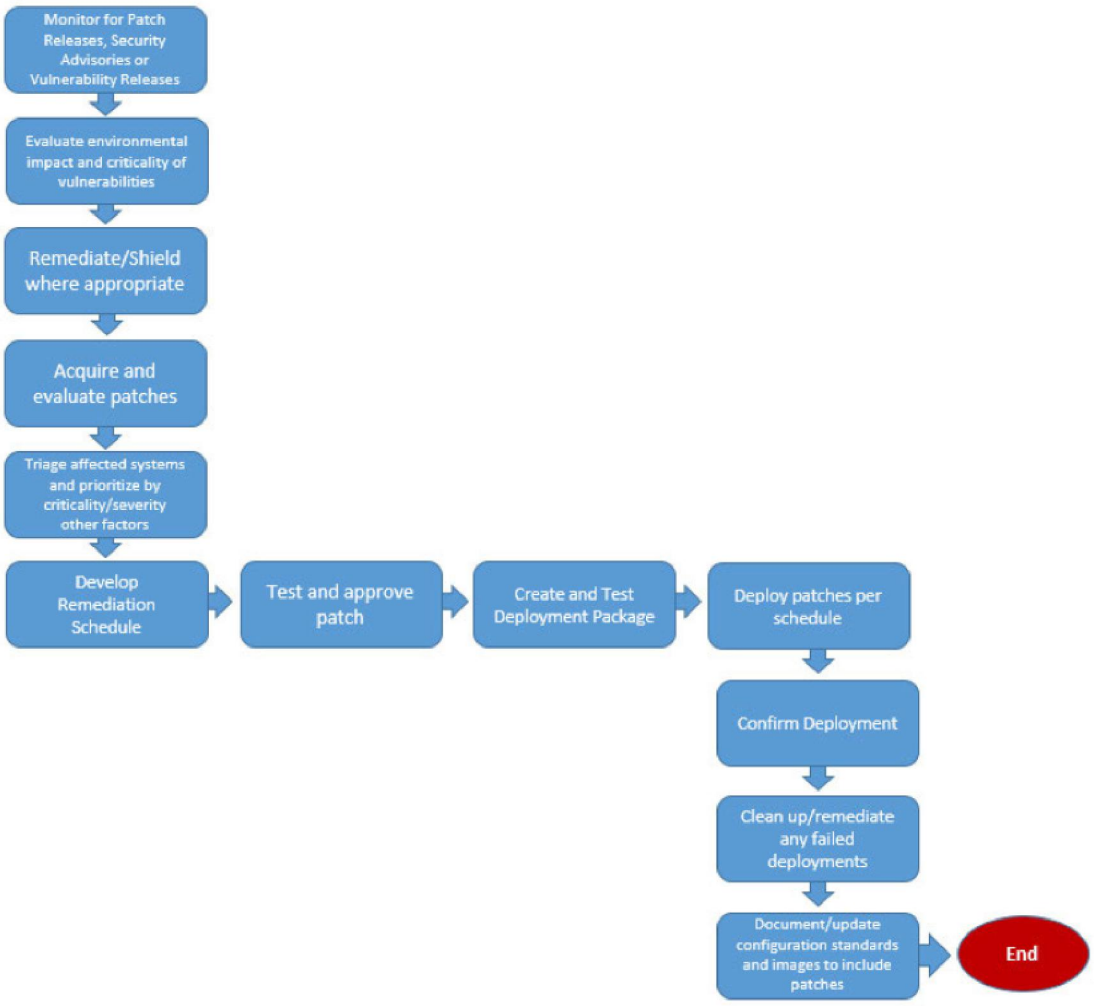


Figure 2 Windows Patch Process

Iron Bow will leverage [redacted] integrated with Iron Bow's SCCM infrastructure to manage non-windows (macOS, iOS, Android) endpoints. As part of Iron Bow's Services, Iron Bow will manage Devices as follows:

Enrollment and management into the solution will be according to, but may not be limited to, the following process:

- Enroll Devices
- Map Devices to groups/categories
- Manage, deploy, monitor and configure apps
- Manage Device configuration and define platform specific policies
- Define actions for Device non-compliance
- Continually monitor Devices for compliance

Iron Bow will, per defined platform specific policies regarding Patching and updates described in the VITA Rules and SMM, perform tasks including :

- Monitor for Patch releases, security advisories or vulnerability releases
- Evaluate Environmental impact and criticality of vulnerabilities and remediate/shield where applicable
- Acquire and evaluate Patches
- Triage affected systems and prioritize by criticality or other factors and develop remediation schedule
- Test and approve Patch
- Create and test deployment package
- Deploy Patches per schedule
- Confirm deployment
- Cleanup/remediate any failed deployments
- Document/update configuration standards and images to include deployed Patches

1. Patch and upgrade End User Devices to required levels in accordance with the SMM.

In performing these functions, Iron Bow will replace old Software versions with new updates, as well as institute a process for deploying them to the enterprise. For this project, Iron Bow will use a set of tools, as described in Section 2.3.1, for Software distribution. SCCM will be used as the Microsoft Software distribution solution. SCCM provides advanced features for deploying and managing Software, Windows Patches, and critical updates. The advanced capabilities of SCCM include, but are not limited to inventory-based targeting, status reporting, server-side and client-side scheduling, multisite facilities, centralized Hardware and Software inventory, remote diagnostic tools, Software metering, Software distribution-point population and maintenance, support for Windows 10 and Office 365 clients, and enhanced Software deployment features. SCCM also integrates with MDT for packaging and Cherwell Service Management and Asset Management. For macOS (OS X), Windows phone, iOS, Android Mobile OS Iron Bow will use [redacted] to Patch and upgrade the Devices as required. To close any gap with 3rd party applications, Iron Bow will also leverage [redacted] for SCCM. [redacted] for SCCM maximizes Iron Bow's investment in SCCM, reducing any security risk from unpatched non-Microsoft third-party applications such as Adobe Acrobat Flash and Reader, Google Chrome, and Mozilla Firefox. [redacted] uses the existing SCCM Patch management infrastructure and console. The plug-in installs in minutes, choosing what to publish from the catalog, with the packages showing up alongside the Microsoft updates. [redacted] also provides Iron Bow increased capability in supporting Patches on Devices that are disconnected from the network.

Security and Patch Information Sources. Iron Bow will provide for the intake and vetting of information regarding both security issues and Patch releases, which will alert the team to security issues and Software updates relevant to VITA. Iron Bow will assign an individual on the EUC Team to be responsible for keeping up-to-date on newly released Patches and security issues that affect the systems and applications deployed in the Environment. This individual will also take the lead in alerting administrators and Users of security issues or updates to the applications and systems used and supported. Iron Bow will determine whether all existing systems are accounted for when researching and processing information on Patches and updates by providing a comprehensive and accurate management system (Cherwell Asset Management) which will be linked to SCCM..

Patch Prioritization and Scheduling. Iron Bow will ensure that scheduling guidelines and plans exist within the Patch management program. First, a Routine Patching Plan will be developed by Iron Bow and will guide the normal application of Patches and updates to systems. This plan does not specifically target security or other critical updates. Instead, this plan is meant to facilitate the application of standard Patch releases and updates. This plan can be time or event based; for example, the schedule can mandate that system updates occur quarterly, or a cycle may be driven by the release of service packs or maintenance releases. In either instance, modifications and customizations will be made based on availability requirements, system criticality, and

available resources. For prioritization, Iron Bow will use the OEM recommendations to develop Patch schedules (see Figures 3, 4 and 5 on the next page) or will prioritize as otherwise required by VITA.

Secondly, a Security Patch Plan will be developed jointly between the VITA and Iron Bow to deal predominantly with critical security and functionality Patches and updates. This plan will assist Iron Bow, the MSS, and VITA in prioritizing and scheduling updates that must be deployed immediately. Iron Bow will consider a number of factors to determine Patch priority and scheduling urgency. Responses to information security and vendor-reported criticality (e.g. high, medium, low) will be key input for calculating a Patch's significance and priority, as is the existence of a known exploit or other malicious code that uses the vulnerability being Patched as an attack vector. Other factors that will be taken into account by Iron Bow when scheduling and prioritizing Patches are system criticality (e.g. the relative importance of the applications and data the system supports to the overall business) and system exposure (e.g. DMZ systems vs. internal file servers vs. client workstations).

Iron Bow will make informed decisions about Patch prioritizations with consideration of the systems which make up the operational Environment, and the potential impact that each one of those systems has on enterprise security. Iron Bow will mitigate the risk this presents by coordinating with VITA, the MSS and the MSI in performing a thorough asset analysis and vulnerability tests to find available systems and associated open vulnerabilities. Each of these Patches will be evaluated and assessed for how it will be prioritized for deployment. Iron Bow will collaborate with the MSS to prioritize Patches based on the risk particular vulnerabilities pose to critical assets, as well as their exploitability and age. Iron Bow's process focuses on the EUC critical assets thereby eliminating vulnerabilities that put those critical assets at risk.

Prioritizing vulnerabilities will require consolidating multiple vulnerability scanner feeds and analyzing issues based on known exploits, as well as simulating potential attack paths through the IT infrastructure. External information sources such as US-CERT TA15-119A - which has the top 30 attack vulnerabilities – will also be used as resources information. The results will be compiled by Iron Bow, in conjunction with the other Towers as defined in the SMM, in the SMS.

Iron Bow will collaborate with VITA, MSI and the MSS to use available severity rating systems from OEMs that rate each vulnerability according to the worst theoretical outcome were that vulnerability to be exploited.

The measure of a vulnerability's severity is distinct from the likelihood of a vulnerability being exploited. To assess that likelihood, as mentioned above, Iron Bow will also look at other risks such as exploitability. For example, the Microsoft Exploitability Index provides additional information to help the Hardware and Software Services Team better prioritize the deployment of Microsoft security updates. This index provides guidance on the likelihood of functioning exploit code being developed for vulnerabilities addressed by Microsoft security updates, within the first 30 days of that update's release. While this severity rating system is intended to provide a broadly objective assessment of each issue, Iron Bow will also evaluate VITA's Environment and make decisions by coordinating with the STSs and VITA about which updates are required to protect their critical systems. Microsoft evaluates the potential exploitability of each vulnerability of important or critical severity associated with a Microsoft security update and then publishes the exploitability information as part of the monthly Microsoft security update details. If, after publishing the details, Microsoft determines that the exploitability index assessment warrants a change, it will change the assessment and notify customers through technical security notifications and Iron Bow will consider such notifications.

2. Provide capability to distribute Patches and updates to subsets of Devices (e.g., by Customer, groups, geographic locations) in accordance with the SMM.

Iron Bow's Patch management policy will provide for Patches that are pre-approved on an ongoing basis, based on conditions defined pursuant to the SMM. Iron Bow's Patch management policy will not only manage the Patches made available in Windows Update but also increase the security of the Device population as a whole

which includes all supported OSs. Iron Bow will have the ability to set up an account-level or site-level policy that can target multiple Devices, define the Patch window, Patch location, automatic approval rules and special options such as reboot behavior. Iron Bow also has the ability to create a Patch management policy for audit purposes only and will provide such as part of the Services. When needed, Iron Bow will also provide the ability to apply site-level overriding of account-level Patch policy options, all in accordance with SMM.

3. Provide ability to exclude specific Devices, or subsets of Devices (e.g., by Customer, groups, geographic location), from specific Patches and updates.

As stated in Section 2.3.3 #2 directly above, the same is true for excluding Devices.

4. Monitor software providers and inform the MSI or VITA as defined in the SMM of the available driver upgrades or Patches suitable/required for End User Devices.

Iron Bow will maintain strategic relationships with VITA's key OS and application OEMs that facilitate the timely release and distribution of information on product security issues and Patches. Iron Bow is currently on vendor security announcement lists, will review security announcement sites and institute monthly calls with the manufacturer representatives to obtain information. In addition, public web sites and mailing lists will also be regularly monitored by Iron Bow's EUC staff. Such information sources include Bugtraq, the various SecurityFocus lists, and Patchmanagement.org. Iron Bow will also utilize their Partner Alliances Team to stay current with each OEM. Iron Bow has personnel assigned to manage the channel relationships for all OEMs in the solution. Because of these relationships, Iron Bow receives alerts/notices of such requirements to include End of Life (EOL) and End of Sale (EOS). Iron Bow will maintain open lines of communication and create a standard reporting mechanism as defined in the SMM to advise MSI or VITA when new driver updates or Patches are available.

5. Maintain and update the list of Software and their Patching categorization in accordance with the SMM and VITA Rules.

To provide a Software Patching program, Iron Bow will first: 1) identify all installed Software products, 2) match installed Software products to existing Software licenses, and 3) report compliance status. Iron Bow will review the existing SOPs in place for managing and maintaining Software licenses. In addition, Iron Bow will review the current Software inventory, Software license inventory, license and maintenance agreements, audits/reconciliations, and prior monthly reports to search for trends and inconsistencies. Using Cherwell as Iron Bow's Asset Management tool linked to SCCM will improve IT governance through stronger Software compliance standards and processes, automated correlation of relevant Software products within the infrastructure to their respective licenses, and reduced costs of license procurement, use rights and Software purchases. In addition to the licensing information, Iron Bow will track Patching categorization in accordance with the SMM and VITA Rules. Iron Bow's categorization will be based on the criticality of the system, data handled, and the complexity of the Environment (e.g. number of supported platforms and applications, number of remote offices).

6. Evaluate each released driver upgrade or Patch for its applicability and criticality and present a recommendation as to when each Patch should be installed on End User Devices.

The breadth and detail of Iron Bow's Patch/driver testing process will relate directly to the applicability and criticality of systems and data handled and the complexity of the Environment (e.g. number of supported platforms and applications, number of remote offices). Iron Bow's Patch/driver testing process will begin with the acquisition of the Software updates and continue through acceptance testing after production deployment. The first component of Patch testing will be the verification of the Patch's source and integrity. This step will help Iron Bow ensure that the update is valid and has not been maliciously or accidentally altered. Digital signatures or a form of checksum or integrity verification will be a component of Patch validation. This signature

will be regularly verified, especially as an update is passed through operations (e.g. on the update server, in build images, in Software repositories). Upon completion of the evaluation process , Iron Bow will make a recommendation to VITA as to when each patch should be installed on the End User Devices.

7. Perform regression / interoperability testing in a lab Environment that reasonably reflects the target Environment to validate that the driver upgrades or Patches will operate as expected and not adversely affect End User Devices following installation.

Iron Bow will perform regression / interoperability testing in a lab Environment that reasonably reflects the target Environment to validate that the driver upgrades or Patches will operate as expected and not adversely affect End User Devices following installation. Once a Patch/driver has been determined valid, it will be placed in a test Environment. Iron Bow will mirror the production Environment as closely as possible. It is important to at least account for the majority of critical applications and supported operating platforms in the Patch testing Environment and Iron Bow will ensure this is the case. There may be instances where a subset of production systems will serve as an ad hoc test Environment; and upon VITA approval Iron Bow will use IT employee systems in these cases. Regardless of the available test equipment and systems, Iron Bow will expose the update to as many variations of production-like systems as possible to ensure a smooth and predictable rollout. All of Iron Bow's testing will be performed in accordance with SMM and VITA Rules and coordinated with the MSI, in addition to other STS as required.

8. Perform additional regression and interoperability testing that may be required for existing End User Device images and Software.

Iron Bow will perform additional regression and interoperability testing that may be required for existing End User Device images and Software. The actual mechanics of testing a Patch/driver may vary widely. This testing may be simply installing a Patch/driver and making sure the system reboots, or the test procedure may involve the execution of a battery of detailed and elaborate test scripts that validate continued system and application functionality. Iron Bow will use a suitable approach toward detailed Patch/driver testing which will be dictated by system criticality and availability requirements, available resources, and Patch severity.

The initial phases of production rollout may be considered an additional component of the testing process. If allowed by VITA, rollouts will be done in tiers, with the initial tiers often involving less critical systems. Based on the performance of these stages of the Patch deployment process, the entire Environment will be updated, and the testing process will be considered finished with the successful completion of final acceptance testing.

All of Iron Bow's testing will be performed in accordance with SMM and VITA Rules and coordinated with the MSI, in addition to other STS as required.

9. Deploy Patches in accordance with the Change Management process defined in the SMM.

All applicable system modifications, Patches and updates will be performed and tracked by Iron Bow through the Change Management System. Iron Bow will use Cherwell's Service Management System which will be integrated with MSI's SMS. Patch application plans submitted through Change Management will have associated contingency and back-out plans if something goes wrong during or as a result of the application of a Patch or update. Also, information on risk mitigation will be included in the Change Management system. Monitoring and acceptance plans will also be included in the Change Management process. Iron Bow will assign specific milestones and acceptance criteria to guide the verification of the Patches' success and to allow for the closure of the update in the Change Management system (e.g. no reported issues within a week of Patch application). Iron Bow will deploy Software, driver, and Patch updates as needed on an emergency basis, to include remote and mobile Users, in accordance with the SMM and VITA Rules.

Iron Bow will assign the most experienced engineers and administrators during the deployment phase of the Patch management process. This stage is the most visible to the organization and will measure the overall

success of the deployment and the Patch management program in total. In determining the use of SCCM as Iron Bow's Patch management tool, Iron Bow considered: the number of platforms supported, the number of systems to be Patched, existing expertise and personnel involved, and the availability of existing system management tools. Iron Bow will apply updates in a controlled and predictable fashion. Iron Bow will recommend as part of policy review that no Customer End User or administrator will arbitrarily apply a Patch. Iron Bow will also discuss with VITA their existing policies for limiting when and by whom Patches are applied. The type of controls enforced will vary by organization and requirement; however, they all include, but are not limited to, items such as restricted User rights (the User does not have sufficient permissions to update the system) and network-based access controls (the system cannot access the resources needed to perform an update). Iron Bow will review the Patch status to determine where failed and evaluate procedure to re-initiate.

10. Automatically execute Software distribution activities to bring Devices into compliance if any or all tracked compliance components are missing in accordance with the SMM and VITA Rules.

Iron Bow's Patch management program will identify Devices that are out of compliance and Iron Bow's goal will be to reduce non-compliance. To supplement post-implementation assessment, Iron Bow will put controls in place to ensure that newly deployed Devices are up to specification with regard to Patch levels.

Based on Iron Bow's past experience, system build tools and guidelines are the primary enforcement means of ensuring compliance with Patch requirements at installation time. As new Patches are approved and deployed, build images and scripts will be updated so that all newly built systems are appropriately Patched, and associated build documentation will be updated to reflect these changes. In addition to updates to build tools and documentation, Iron Bow will provide and follow operational procedures to facilitate ongoing compliance of newly built systems. Changes will be handled via a Request for Change through the MSI's SMS. Any new Patches and updates that are approved and installed will also be integrated by the engineering team into new builds and recorded in the Change Management system to provide both an appropriate audit trail and suitable procedural guidelines.

For any system deemed to be out of compliance and the End User has been provided an opportunity to self-deploy and missed the deadline, an ADR will automatically push the Patch.

11. Report on systems remediated in coordination with MSI.

Regular audit and assessment will allow Iron Bow to gauge the success and extent of Patch management efforts. There are 2 critical success factors to audit and assessment: accurate and effective asset and host management. Often, asset and host management are conducted through the use of a single product, such as SCCM. Our SMS system, Cherwell Service Management will be integrated with all support tools and will allow Iron Bow to accurately track deployed Hardware and Software throughout the enterprise, including remote Users and office locations. These tools will also allow Iron Bow administrators to generate reports (e.g. all End Users without a given hot fix, all versions of particular applications) that Iron Bow will use to deliver consistent installation of Patches and updates across the organization.

Device discovery and auditing are also components of the audit and assessment process. While asset and host management systems will help Iron Bow to administer and report on known systems, there are likely a number of Devices that have been either unknowingly or intentionally excluded from inventory databases and management infrastructures. Iron Bow will use Device discovery tools to uncover these Devices and assist in bringing them under formal system management and Patch compliance.

Iron bow will report on systems remediated in coordination with the MSI.

2.3.4 Software Evaluation

1. Provide Software consultation services, to include:

Iron Bow will provide subject matter expertise on services that include, but are not limited to: assess and advise whether a product can be packaged; assess and advise whether the product can be installed on any VITA OS; assess and advise whether the product can be installed on VITA standard Hardware; and assess and advise whether the product can coexist with all core Software installed on the End User Devices to which this product will be installed.

2. Assess and advise whether a product can be packaged.

Application packaging involves the preparation of standard, structured Software installations targeted for automated deployment. Iron Bow will assess and advise whether the automated installations, or packages, meet the installation requirements for a specific Environment. Such assessment will include a review of VITA standards for Software usage and desktop design, regional issues, and Software-related support issues. In addition, packages will be prepared for both commercial-off-the-shelf (COTS) Software and applications developed in-house.

Iron Bow may find that certain applications should be deployed outside an automated Software distribution. Through consultation with VITA and the MSI, Iron Bow will establish a structure for classifying and managing diverse Software used throughout the enterprise and use alternate patching methodologies as may be required.

3. Assess and advise whether the product can be installed on VITA standard OS.

Iron Bow engineers will not begin packaging until the baseline image has been reviewed and approved by VITA. Iron Bow will assess and advise whether the automated installations, or packages, meet the installation requirements for the VITA-specific Environment to include OS.

4. Assess and advise whether the product can be installed on VITA standard Hardware.

Iron Bow will assess and advise whether the automated installations, or packages, meet the installation requirements for the VITA-specific Environment to include Hardware. Iron Bow will not install the baseline image prior to VITA's acceptance of such.

5. Assess and advise whether the product can coexist with all core Software that will be installed on the End User Devices to which this product will be installed.

Iron Bow will identify conflicts between old and new applications, and use a structured method for resolving the conflicts. MDT allows Iron Bow to quickly identify common conflicts and then aid in establishing policies for conflict resolution as well as for automating the conflict-management process.

2.4 Hardware Services

1. Provide Hardware that underpins EUS solutions, including: laptops, desktops, tablets, monitors, docking stations, and associated peripherals and cables.

Iron Bow has chosen to develop Hardware-only Resource Units (RUs) as the foundation of the EUC solution. Iron Bow offers a variety of base Devices including laptops, desktops, tablets, and ruggedized Devices from a variety of OEMs (including Apple, Dell, HP, and Microsoft). All Device RUs include power cords and batteries in addition to standard OEM extended warranty/maintenance coverage for the term of the service. Additionally, desktop RUs include 1 of each: monitor, keyboard, and mouse. Two and three year refresh terms have been provided for all tablets, convertible, detachable and ruggedized devices. Three year refresh terms have been provided for all laptops. Four year refresh terms have been provided for all desktops.

It is important to note that Iron Bow has direct partnerships with over 500 IT OEMs and access to over 17,000 OEMs through multiple distribution sources. Significant buying power and worldwide support capabilities enable Iron Bow to hold the highest-level certifications with many tier one OEMs. Iron Bow's internal product database currently contains over 5,000,000 products from over 3,000 OEMs. Iron Bow's catalogs are synchronized on a

regular schedule with three top IT distributors, Synnex, Arrow and Ingram Micro, and with Iron Bow's top 20 OEM partners. Therefore, Iron Bow has the ability to provide the Commonwealth with a broad range of Devices upon request from VITA and/or to be added through the technical refresh process.

All products provided will be new.

2. Provide Hardware from a variety of manufacturers for all classes of End User Devices (e.g., HP, Dell, Lenovo, Apple, Microsoft, etc.).

Iron Bow's Hardware RU's include laptops, desktops, tablets, ruggedized Devices, and thin clients from HP, Dell, Apple, and Microsoft. Throughout contract performance, Iron Bow will continuously refresh Device offerings and can add additional OEM's as requested by VITA through the technical refresh process. The technical refresh process will be maintained in the SMM. Iron Bow's Quality Assurance and Service Catalog Manager will work with VITA and the Agencies to define use cases and develop the most appropriate solution to meet End User's needs.

3. Provide capability to source and provision all VITA approved Devices in all VITA locations.

Iron Bow will maintain top tier partner status with key industry OEMs including HP, Dell, Apple, and Microsoft. Iron Bow will only resell OEM authorized products procured through a secure supply chain which encompasses OEMs and authorized distribution partners (e.g. Synnex, Arrow, Ingram Micro, and Tech Data).

4. Test all new End User Device models and provide a "certified" status to the VITA upon completion.

Iron Bow will test End User Devices within Iron Bow's lab for form, fit, and function. The certification process for the Devices will be defined in the SMM. Upon satisfactory completion and "certified" status, notice will be provided to VITA.

2.4.1 Product Selection

1. Work with MSI to populate the Service Catalog which provides a level of choice to satisfy Customer business needs. At a minimum, this should include:

Iron Bow will collaborate with the MSI during the Service Catalog Management process. Iron Bow will work with the MSI to ensure that items for EUC are complete and properly describe the Hardware and/or Service and the process used to enable the product or Service. Adding new or changing items to the Service Catalog will be in accordance with the process described in the SMM.

A variety of additional peripherals have been added as separately purchased items to allow VITA to maximize choices and offer flexibility to Agencies. These peripherals are available for purchase for Customers and will not be rolled into the monthly unit price of the EUC Device. The peripheral list will be adjusted upon request from VITA and/or through the technology refresh process, as documented in the SMM.

1.1 A variety of types of End User Devices, with a range of capabilities: laptops, desktops, tablets.

Iron Bow will work with the MSI to populate the Service Catalog with the RUs. Iron Bow will offer a set of Premium, Performance, and Standard Laptops; Performance, Standard, and Basic Desktops, Convertible and Detachable Tablets, and Ruggedized Devices. Throughout contract execution, Iron Bow's Quality Assurance and Service Catalog Manager will work with VITA and the MSI to refresh the Hardware offerings as required, and then use the data to populate the Service Catalog maintained by the MSI.

1.2 A variety of OS, including: Windows, OSX, Linux, iOS, Android, Linux, ChromeOS.

Iron Bow's current offerings include Windows, Linux, Andriod, ChromeOS, macOS and iOS OS's. Throughout contract execution, Iron Bow's Service Quality Assurance and Service Catalog Manager will work with VITA and the MSI to refresh the Hardware offerings to include all desired OS. Iron Bow will source and deploy systems with all of these OS's. Detailed specifications for each RU are provided in the RU description (see Exhibit 4.2).

1.3 Features that such as touch screen capability, cameras, mobile (cellular) connectivity, etc.

The current set of RU's represent standard features and functionality, and have Devices that include additional features such as enhanced graphics capability, touchscreen capability, cameras, Bluetooth, webcams, microphones, and cellular capability if not already standard. Additionally, Iron Bow has included Microsoft Surface tablets that are cell enabled and Wi-Fi capable and/or Wi-Fi only.

1.4 A variety of peripherals, including: cables, monitors of varying sizes, docking stations, mice, keyboards, extended batteries.

Iron Bow's solution includes a variety of peripherals from various OEMs such as cables, monitors, docking stations, mice, keyboards, replacement batteries and extended battery warranties. Peripheral Devices are separate and discrete Devices that can be purchased by end users to complement their Device RU.

All peripherals ordered through the Service Catalog will be installed and supported by Iron Bow pursuant to established SLAs. Iron Bow Field Service Technicians will provide best effort in supporting peripherals not ordered through the Service Catalog. Service for peripherals not ordered through the Service Catalog will not be covered under SLAs.

For those peripherals not having an OEM warranty, Iron Bow will offer a 90-day warranty when the peripherals are ordered directly from Iron Bow. Peripherals ordered as part of a Desktop bundle, will have the same warranty as the desktop bundle. Warranty claims will be handled by Iron Bow.

The peripheral offering is organized into two primary categories:

1) System/category Specific: Where Iron Bow has identified specific peripherals for specific set of RU Devices, they are presented as a group for ease of ordering. For example, there is a set of peripherals specifically for the Dell Latitude 14 Rugged 5414. Similarly, where peripherals are valid and compatible with a broader group of Device RUs, these are listed together. For example, there is a broad array of Microsoft Surface Pro Peripherals and Apple Laptop Peripherals.
2) System agnostic: System agnostic / OEM agnostic peripherals are compatible with any Device RU and represent useful accessories for VITA Customers. This includes sets of general peripherals such as universal docking stations.

Iron Bow will utilize the technical refresh process, as described in the SMM, to update the peripherals list throughout the life of the contract. Iron Bow will add peripherals to the Service Catalog in accordance with the MSI's Change Management procedures and technical refresh process as documented in the SMM.

1.5 Peripherals as may be required to support accessibility features.

Peripherals required to support accessibility features, are included in Exhibit 4.1. Iron Bow will follow the technology refresh process, as documented in the SMM, to add peripherals on an a-la-cart basis, and/or bundle new peripherals with the Devices offered.

1.6 A variety of performance options (e.g., CPU, RAM, storage size, etc.).

Each of the various form factors included in Iron Bow's RU's provide a varying level of performance options to accommodate a variety of use cases. CPU's range from i3 to i7 and RAM ranges from 8 GB to 512GB depending on the Device. The peripheral list also includes upgraded RAM and Hard Drives for available systems with their desired processor and hard drive size.

2. Work with VITA and other VITA designees to evaluate price, Hardware components, warranty, service history, and availability as part of End User Device selection determination.

Iron Bow's Quality Assurance and Service Catalog Manager, in coordination with the Program Director, will work with VITA, its designees, and the OEMs to evaluate price, Hardware components, warranty, service history, and availability as part of the End User Device selection process. Iron Bow has a highly certified, solutions-focused engineering staff who are responsible for understanding today's technology and tracking and projecting the evolution of future technologies. Iron Bow corporate resources will assist during Implementation with the development and review of functional and technical requirements and develop solutions in coordination with Iron Bow's OEM partners to meet End User's needs. Continuing technical refresh activities will be performed post Commencement in accordance with the technology refresh plan, as documented in the SMM.

3. Ensure End User Device Hardware properly supports appropriate VITA-approved Operating Systems and Software in accordance with the SMM and VITA Rules.

As new products are added to the catalog, Iron Bow's Service Catalog Team will ensure the proposed Devices are thoroughly vetted through the following process a) obtain demo gear from the OEM's; b) prepare test plans to thoroughly document the applications and features that will be tested; c) execute testing in Iron Bow's lab; d) document test results; and e) obtain VITA approval to add the tested and approved Devices to the Service Catalog. The detailed test process will be included in the technology refresh plan, as documented in the SMM.

4. Provide proof of concept or test Devices on a non-chargeable basis, including to Customers or other suppliers as required.

Iron Bow's relationships with the OEM's provides access to proof of concept and/or test Devices that will be utilized to validate functional and technical requirements for new solutions. Iron Bow will provide such devices to Customers for testing, as well as perform testing in the Iron Bow lab. All of Iron Bow's testing will be performed in accordance with SMM and VITA Rules and coordinated with the MSI, in addition to other STS as required.

5. Ensure Hardware offerings comply with VITA Rules, architecture standards, and Hardware manufacture recommendations.

VITA Rules, architecture standards and OEM recommendations were considered as Iron Bow developed the final Hardware offerings and will also be considered during the technical refresh process to ensure offerings comply with VITA Rules, architecture standards and Hardware manufacturer recommendations. Iron Bow's Quality Assurance and Service Catalog Manager will ensure compliance is documented and maintained as new items are reviewed for approval to be added to the Service Catalog.

6. Continually evolve Hardware offerings with current standards in the marketplace.

Iron Bow is dedicated to helping VITA make informed technology decisions that satisfy near term requirements while supporting long range goals. Iron Bow will leverage close relationships with all industry-leading IT OEMs (including Apple, Dell, HP, and Microsoft) to provide VITA with product roadmaps, advanced technology briefings, equipment for in-house evaluation, and access to Iron Bow and OEM lab and test facilities. This will provide VITA with the expertise required to make informed IT purchasing decisions.

Benchmarking is the act of running a computer through a series of predetermined tests or program operations to assess its overall performance. Iron Bow will perform benchmarking in order to gauge the performance of the Hardware to ensure it is performing as designed. Through benchmarking, Iron Bow will compare Hardware performance relative to other computers. Iron Bow will use a variety of ways to benchmark a PC, with specific methods focusing on the PC as a whole, or specific components, such as the graphics card, CPU, or SSD.

In addition to in-depth OEM information and resources, Iron Bow will provide pragmatic, OEM independent information and recommendations including:

- Preparing and providing periodic "Technology Assessments" tailored to the Commonwealth's Environment and requirements
- Providing high level technical analysis by technology consultants experienced with the Commonwealth's Environment
- Maintaining a working test lab capable of testing Hardware and Software products prior to their consideration for integration into the Commonwealth's Environment
- Providing insight into emerging technologies that may become available in the near future.

OEM and distributorship partnerships provide Iron Bow with access to virtually every IT OEM and product available. This allows Iron Bow to quickly add products to the contract. In collaboration with VITA, the MSI and Customers, Iron Bow will provide the following services to continually evolve Hardware offerings with current standards in the marketplace

Platform Selection and Evaluation. Iron Bow recognizes that VITA requires a comprehensive Service Catalog that encapsulates the varying needs and demands across all the Agencies operating within the Commonwealth of Virginia. Iron Bow has a dedicated team of EUC personnel who will manage the Service Catalog in a proactive manner to ensure its representative of not only a flexible set of offerings, but also accurate in regards to presenting options that are readily available and in line with expectations surrounding supportability, warranty and performance. Iron Bow will utilize the following controls and strategies to assist with the successful delivery and ongoing management of the Service Catalog:

a. **Product Obsolescence Management**. Iron Bow will perform ongoing audits and reviews of the service catalog's offerings to ensure it is up to date. The goals of these recurring audits are to identify offerings that are nearing their EOL/EOS dates, with the standard being to identify any products that are 6 months away from such a date. Those offerings found to be in that range will then go through a comprehensive technology refresh process, as described in the SMM, in order to identify viable replacement offerings and a resultant refresh of the catalog. Iron Bow fully understands that the proposed product must receive final approval by VITA, before any such refresh of the catalog occurs.

b. **Service Catalog Lifecycle Management**. Iron Bow recognizes and understands that the Commonwealth is comprised of diverse Agencies whose individual missions may require the use of Device configurations which may or may not align with VITA's standard Device offerings. As such, Iron Bow will support the addition and maintenance of any ad-hoc or customized configurations deemed necessary by VITA.

   In order to support all User populations and to ensure VITA has the latest Device options available in the Iron Bow Service Catalog, Iron Bow is proposing the following draft Device lifecycle management strategy which will be submitted for VITA's acceptance:

   - Upon Effective Date, Iron Bow will work with VITA to proactively identify Agencies carrying the potential for specialized technical requirements and/or configuration needs
     - Iron Bow will meet with such identified Agencies in order to better capture the types of specialized requirements that may exist and that need to be offered through Iron Bow's catalog
     - All customized configurations will be added to the Service Catalog once properly vetted out
   - Iron Bow will proactively schedule quarterly requirements and configuration review sessions with VITA and any relative or necessary Agency contacts to cover the following items:
     - Review technical requirements relative to the evolving OEM platforms which are available and applicable to each agency use case
     - Present and review findings from the latest product obsolescence management process

- Present any desired technology roadmaps for each OEM represented in the catalog as well as any new ones being considered for addition.
- Discuss catalog refresh strategies and suggested updates based on the results and feedback from the above mentioned sessions
- Catalog changes will be documented and communicated to VITA for approval prior to being populated into the Service Catalog

In order to provide maximum flexibility associated with the catalog while also ensuring the proper procurement controls are in place, Iron Bow will implement the following:

- User profiles will be aligned with their organizational role within the Service Catalog logic so they will only be able to see Device options which are appropriate for their job function and/or agency specific guidelines
- Iron Bow will create a customized set of RUs which allow predefined Users the ability to customize their Device(s) during the ordering process
- Customization limitations will be determined ahead of time so that the flexibility of customization is experienced by Users while on the back end there are still controls to limit the level of customization
- Iron Bow will allow for mid-cycle refresh procurements in case Users have an approved role change or event which requires them to obtain a new Device prior to the normal refresh cycle

Iron Bow's program management team understands that achieving successful technology enhancements for Customers relies heavily on providing strict accountability, continuity of operations and zero degradation of services. To achieve this goal, Iron Bow has developed a comprehensive, process-based approach. Iron Bow's program management team will apply this methodology in order to properly control the rollout of technologies and ensure a high level of end User satisfaction. Included in this approach is a continually updated repository of procedures and processes for implementing, managing and guiding the delivery of enhanced technologies. Iron Bow will:

- Work collaboratively with the MSI, VITA and the Agencies involved to determine if any enhancements to the rollout process are necessary, integrate them and any new staff into the operation and ensure the continuation of daily operations to client's satisfaction
- Establish a solid base for a high-quality, long-term contractor/client relationship at both the working and at the senior management level
- Implement integrated management, operational and quality control processes as required, that properly align with the MSI, VITA, and the Customer's current procedures and processes
- Avoid unscheduled disruptions to Customer's current operation
- Identify and manage risks associated with the Implementation; and apply critical success factors and lessons learned from recent implementations.

This plan maximizes the process for announcing changes in a timely manner, for providing timelines, dependencies, etc. for replacement components, and for working with the Commonwealth to initiate those changes over the life of the contract. Furthermore, this plan presents a strategy/methodology to manage Hardware and Software obsolescence, which includes a process to notify the Commonwealth when any item nears EOS and EOL and proposal of replacement components/Devices that mitigate the impact on standard solution configurations and/or the OEM list of products.

Iron Bow will identify items that are nearing EOS or EOL and will propose to VITA replacement items for addition to the Service Catalog. Iron Bow will only add VITA-approved items. Changes may be the result of recommendations made by Iron Bow in the EOS/EOL Reports and as a result of the above described quarterly reviews.

Iron Bow's technology refresh and obsolescence management strategy is designed to enable a proactive approach to identify, schedule, and update operational IT Hardware and avoid obsolescence. Iron Bow will stay abreast of OEM plans for Hardware and Software evolution. Iron Bow's Service Catalog Team will develop technology refresh proposals based on end User feedback and involvement, thus increasing the chances that what is ultimately delivered to the end-User meets their needs. This plan maximizes the process for announcing changes in a timely manner, providing timelines and dependencies for replacement components, and working with VITA to initiate those changes over the life of the contract. Furthermore, this approach offers a strategy and methodology to manage Hardware and Software obsolescence, which includes a process to notify VITA when any item nears EOS/EOL, and proposal of replacement components or Devices that mitigate the impact on standard solution configurations or the OEM product list. Iron Bow will notify VITA when any item nears EOS or EOL, with the standard being to identify any products that are 6 months away from such a date.

c. **Technical Refresh and Alternative Solutions**. Iron Bow will support a variety of approaches in managing and maintaining the catalog. Iron Bow will evaluate new technical solutions as soon as they are commercially available.

   Iron Bow's Partner Alliance Team maintains close working relationships with each OEM, supplier and subcontractor with which Iron Bow engages. These relationships provide Iron Bow with advanced knowledge of both OEM product releases and OEM strategic and tactical directions. This ensures timely and accurate communications to customers on items such as Software bugs, security concerns, product releases, technology obsolescence, new trends in IT and various other OEM announcements. Iron Bow will provide manufacturer based technology roadmaps to assist VITA with technology refresh planning as well as access to technology subject matter experts for further unbiased opinions on the topic. This will allow VITA to make informed purchasing decisions, which maximizes contract value for the agency. Iron Bow will notify VITA when a product will no longer be sold by the OEM and will seek guidance on whether to release pending orders early or to hold orders.

d. **Quarterly Technology Reviews**: Iron Bow is committed to providing the highest quality technical support to the VITA Program Management Office (PMO). Corporately, Iron Bow brings a set of highly certified, solutions-focused engineers and architects who are organized into a series of Technology Practices; these corporate resources are responsible for understanding today's technology and tracking and projecting the evolution of future technologies. These Technology Practices include Networking, Information Security, Secure Mobility, Collaboration (AV), Data Center, and Cloud Computing (including Infrastructure as a Service [IaaS], and Software as a Service [SaaS]); and the engineers who comprise these Technology Practices will be available to review Hardware standards on a quarterly basis with EUC staff, the MSI and/or VITA.

   Iron Bow's Technology Practices will support the PMO by developing and presenting quarterly briefings to key VITA PMO staff on technology trends and emerging technologies. Customized and specific briefings will also be available upon request, and coordinated through Iron Bow's Program Director.

   Iron Bow briefings will provide the pragmatic, OEM independent information and recommendations Customers need to make informed decisions. As these briefings may also include emerging technologies, Customers may be required by OEMs to sign a non-disclosure statement, in which case Iron Bow will take responsibility for facilitating the completion of any NDAs as necessary.

   Additionally, as a continuous service to Customers, Iron Bow will provide ongoing technical value by:

   - Providing "pre-release non-disclosure" information from key manufacturers on new technologies that affect installed systems and systems under development

- Preparing and providing periodic "Technology Assessments" tailored to the specific customer Environments and requirements
- Providing high level technical analysis by pre-sales engineering personnel experienced with the Agency Environments
- Maintaining a working interoperability lab to testing Hardware and Software products prior to their consideration for integration into the Agency Environment
- Providing insight into emerging technologies that may become available in the near future.

7. Ensure products and drivers support minimum of 64-bit architecture OS.

Our Hardware RU's support minimum of 64-bit architecture OS.

8. Provide Hardware-based flexible multifactor authentication (e.g., Intel Authenticate).

Iron Bow will collaborate with the MSI, MSS and VITA to determine a method for multifactor authentication. Iron Bow understands that options may include \ external PIV card reader, external thumb print scanner, and RSA tokens. Iron Bow laptops and desktops come with integrated FIPS-201 approved smart card readers.

2.4.2 Refresh and Replacement

1. Provide multiple service Refresh options (e.g., Two-year, Three-year, Four-Year), which may vary by Device.

Iron Bow's Service Catalog includes 2, 3, and 4-year refresh options to provide maximum flexibility for Customers depending on their needs. Note that the available refresh term varies depending on the type of Device.

2. As a component of the Currency Plan, develop a Refresh plan for all End User Devices.

In collaboration with, and coordinated through the MSI, Iron Bow will maintain the Technical Currency of the EUC Environment. Iron Bow will:

a. Have responsibility from the beginning to the end of Refresh activities through the Refresh process and end with removal and disposal of the assets
b. Acquire all incumbent assets in transit, on order, at configuration center, and at Agency locations awaiting install; Assessment of Hardware will begin immediately after Service Commencement.
c. Continue refreshing assets previously scheduled and waiting to be deployed
d. Be responsible for all scheduling and communication regarding Refresh activities, including End User level communication
e. Adhere to the Release and Deployment Management and Service Validity and Testing for Hardware and Software prior to being introduced to ensure compatibility with Environment

Iron Bow's Program Management Team will participate in the development and management of the Currency Plan, to include the Refresh Plan. The Currency Plan will detail how the Iron Bow will ensure continual Technical Currency of items including systems, tools, deployed assets and the Software and systems residing on deployed assets. At Service Commencement Date, the Iron Bow Program Director and Software and Hardware Services Manager will perform an assessment of the existing assets. Iron Bow will collaborate with the MSI and VITA during such assessment. Based on the results of this assessment, Iron Bow will work with MSI to deliver the initial recommendations regarding such assets to VITA within 30 days after the review.

Iron Bow will provide for Refresh of the legacy assets as agreed to by VITA and in accordance with **Section 8.1.3 of the Agreement**. Iron Bow will prioritize the refresh of legacy assets on an oldest first basis.

The PC Refresh Manager will develop and execute a Currency Plan that moves from takeover in place to the contracted Refresh process. The plan will be presented to and approved by VITA and be fully implemented by March 1, 2019. Activities will include, but are not limited to:

a. Reviewing PC assets in the CMDB, reviewing Service initiation dates and planned Refresh date to determine which are in the most need of Refresh
   i. Oldest assets will be scheduled first
b. Develop Currency Plan in coordination with the MSI to document the Refresh process
   i. Submitted to VITA for approval within 30 days of Service Commencement
   ii. Include process for Service Requests for PC Refresh
   iii. Include process to handle Agencies that are not timely with Hardware and service decisions and build an escalation path for VITA to make selections on their behalf
c. Socialization of the Currency Plan process with Customers will begin immediately after VITA approval. Communication to Customers includes:
   i. Description of new solution – Hardware and Service options
   ii. Sets Agency and User expectations within Currency Planning
   iii. Provide a process for Website and MSI portal notifications
   iv. Schedule for meetings with Agencies
   v. End User training availability and how to request
   vi. Ability for VITA to make on-demand requests for refresh in instances that include but are not limited to: Customer service issues and administration changes.

Iron Bow's Service Operations Manager and PC Refresh Manager will provide data to the MSI to track and report on the completion progress of the Currency Plan. All Refreshes are recorded and reported such that the old and new assets are linked and reported together. Old assets and new assets are represented in the same report or line and associated so it is clear which asset replaced the other and when.

Status/Progress reporting will be clear and concise and shows all status of the assets as they move thru the Refresh process. All reporting will be reconciled to add up to the total number eligible (so that nothing disappears from control/view of VITA/Agencies). Reporting will include:

a. Total assets in CMDB
b. Total assets eligible for refresh
c. Total assets confirmed
d. Total assets ordered
e. Total assets configured
f. Total assets shipped
g. Total assets delivered
h. Total assets installed
i. Total assets delayed

Iron Bow will use Cherwell Asset Management to update the CMDB with Refresh and connected monitor information. Links will be made to show relationships between products, services, and users (parent-child).

Additional views for reporting for VITA or specific Agency Customers include:

a. Total refreshes completed by Agency for the contract period, by year
b. Total refreshes completed by Agency exceeding SLA
c. Total refreshes completed by Agency outside SLA

i. Reason for missed SLA
ii. Actions taken

d. Refresh schedule for the next 12 months
e. Number of Hardware assets that were refreshed
f. Number of Software versions updated
g. Number of open source or free licenses (or similar)

Iron Bow will develop a schedule that focuses on efficiency and constant communication with the Customer to complete the process while maintaining business continuity.

3. Perform on-demand out of cycle End User Device Refreshes.

If requested by an End User, Iron Bow's EUC Team will perform on-demand, out of cycle End User Device Refreshes. These requests will be handled through a Service Request through the MSI's Portal/SMS.

4. When performing End User Device refreshes, migrate all data, configurations, and Software, with the goal of leaving the new End User Device in an equal or better state than the old Device.

Iron Bow will execute PC Refresh activities utilizing EUC Field Service Technicians in combination with a supplemental group of personnel that are solely responsible for supporting PC Refresh surge requirements. Iron Bow will incorporate an updated PC Refresh Procedure in the SMM and will utilize Iron Bow's Quality Assurance Team to continuously improve the work flow management of accomplishing the PC Refresh activities. Iron Bow will ensure the End User Device is in an equal or better state than the old device.

5. Ensure that no End User Devices are outside of OEM support, except as approved by VITA.

Iron Bow's Hardware RU's include standard OEM extended warranty/maintenance support for the duration of the proposed term (2, 3, or 4 years). For example, if a Customer selects a 3 year, premium laptop RU, the premium laptop Device is covered by 3-years of OEM extended maintenance. Iron Bow will work with VITA to determine how to provide this support for legacy Devices that do not have an available OEM warranty.

6. Supplier will Refresh Devices which will maximize the benefit for VITA and Customers (the oldest Devices and those with the highest business impact shall have Refresh priority) while minimizing the business disruption caused by the Refresh.

During Implementation and after Commencement, Iron Bow will use data on the age of each Device to prioritize the first set of refreshes.

7. Within the term of the refresh cycle, repair or replace failed, damaged, or failing components, including:

Iron Bow's Hardware RU's include the following items which will be refreshed when the system is refreshed.

7.1 Peripherals (e.g., mice, keyboards, monitors, etc.)

As previously stated, some peripherals are included with the Device Bundles. Bundled peripherals include mice, keyboards, and monitors for Desktop Bundles. When the Desktop Bundle is refreshed, the monitor, mouse, and keyboard will also be refreshed.

7.2 Batteries

All RU Devices, with the exception of desktops, come equipped with a battery. Iron Bow will provide spare batteries listed as Peripherals for Customer purchase at any time. Iron Bow will provide VITA with 2 options for supporting the replacement of batteries over the life of the contract:

Option 1 => Customer selects their desired battery upgrade/refresh from the peripheral list which allows end users to buy a new battery when they feel their existing RU Device battery no longer meets their needs.

Option 2 => Iron Bow will provide VIP and Gold Service Level End Users with 1 free battery replacement during the life of the system. The End User will submit a Service Request for free battery replacement through the SMS. When assigned to Iron Bow, the Field Service Technician will ship or deliver the new battery per the Service Request.

Iron Bow will also maintain a spare pool of batteries for emergencies at Iron Bow's warehouse locations. Batteries will be replaced when the Device is refreshed.

7.3 Power cords/AC adapters

All Devices come equipped with a power cord/AC adapter. Spare power cords/AC adapters will be maintained at the depot warehouse; power cords/AC adapters will be replaced when the Device is refreshed.

7.4 Cables (e.g., network Patch Cables, video cables, USB)

Cables required to operate the Device come standard with the Device. Spare cables will be maintained at the depot warehouse in case they need to be replaced out of the refresh period; cables will be replaced when the Device is refreshed.

8. Short-term Device Deployment
   Iron Bow will provide a warehouse facility to store Devices that have additional service life. Agencies will open a Service Request for their specific Device needs and duration which will be assigned to Iron Bow. Iron Bow will fulfill the request with existing surplus inventory. For the duration requested, the Agency will pick a Service Level (VIP, Gold, Silver, or Bronze) that will be charged as long as the Device is in use, combined with the monthly Device charge per the Service Catalog. When Agencies are ready to turn in the Device, a Service Request is generated to return the Device back to the warehouse. The Devices will be deployed using the Hard IMAC or Project IMAC process.
9. Device Purchase (Upfront Payment)
   VITA has an occasional need to pay for EUC Devices outright (in advance, with no interest) instead of as a monthly charge due to grant requirements, federal regulations. Device purchase (upfront payment) will be submitted by the Agency through a Solution Request via the SMS. After assignment to Iron Bow, a proposal will be generated outlining the purchase price for each Device and will be based on a quote from the OEM, in addition to Service pricing. Service pricing will either be monthly or calculated as a total price paid upfront by the Agency (Monthly Service Price * # of months = Upfront Service Cost). The Solution Request will follow the workflow and approvals established within the SMM. The Device Refresh will be addressed in the Solution Request proposal according to the terms and duration of the grant.
10. Offline Service Status
    VITA has an occasional need to "shelve" Devices (place them in offline storage), both EUC and Agency-owned, for short periods (ex: VDOT has a large number of tablets used almost exclusively by snowplow drivers during winter months only). A Service Request will be submitted by the Agency for the offline service status via the SMS to deactivate the Device. The monthly Service cost will be reduced to a lower price pursuant to RU established in Exhibit 4.2 regardless of Service Level (VIP, Gold, Silver, or Bronze) for the period of deactivation. A Service Request will be submitted by the Agency via the SMS to reactivate the Device. After assignment, Iron Bow will ensure that all Devices are updated/Patched prior to bringing them online. The Devices will be deployed using the IMAC process.

2.5 Security

Iron Bow will collaborate with the MSS to support multi layered security architectures that include intrusion detection and prevention. Iron Bow will use a variety of techniques to identify normal application behavior, including web applications, and then apply security policies according to VITA Rules. Desktops and laptops will be protected by a comprehensive security solution that includes: antivirus, antispyware, firewall, intrusion detection, and additional scanning capabilities. As discussed in Section 2.5 #7, Hardware or Software authentication mechanisms will be used in the solution. Iron Bow will also provide for the analysis of log files which will be collected, consolidated, and then submitted to the MSS for analysis.

Iron Bow will provide support and assistance to ensure VITA's posture is secure. This includes direct access to Iron Bow's subject matter expertise – such as double and triple Certified Cisco Internetworking Experts (CCIEs), Certified Ethical Hackers, etc. – as well as Iron Bow's vendor partners such as Palo Alto, McAfee, Tenable, Splunk, Qmulos, and Cisco.

1. Ensure Devices are encrypted and functioning for use by Customers in accordance with the SMM and VITA Rules.

Iron Bow will utilize MSS provided security tool's file and disk encryption capabilities to encrypt Devices according to SMM and VITA Rules.

2. Ensure that End User Devices are properly configured and functioning with all required security Software and Device configurations, per VITA Rules and in accordance with the SMM, prior to releasing to Customers.

Iron Bow will use the MSS provide security tool to provide end computer security according to VITA Rules.

3. Ensure correct rights and permissions to End User Devices and related tools are assigned in accordance with the SMM and VITA Rules.

Group Policy is the primary tool used for defining and controlling how Software, network resources, and the OS function for Users and computers. In Active Directory, Group Policy is applied to Users or computers on the basis of their User or computer accounts that exist in sites, domains, or organizational units. Users and computers are the only types of Active Directory objects that receive policy.

4. Identify Users who are no longer with the Supplier and ensure that access privileges are removed in accordance with the SMM and VITA Rules.

Iron Bow has explicit personnel security requirements incorporated within our Standards of Conduct that cover personnel working at corporate and Customer facilities with credentials, badges, or information system privileges. Iron Bow will review these policies to ensure they meet or exceed the SMM and VITA Rules. These policies will ensure appropriate termination of employee privileges and credentials upon transfer or exit from their position. The Iron Bow policy requires exit interviews, guided by a checklist, to ensure terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics at exit interviews include reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Coordination between the Iron Bow PMO, Facility Security Officer and Customer Security is imperative, as timely execution of termination actions is essential for individuals terminated for cause. In certain situations, Iron Bow will consider disabling the information system accounts of individuals that are being terminated prior to the individual's being notified. Iron Bow will coordinate any such activities with Customers, other STS, and VITA as required.

5. Ensure personnel are trained in Security requirements within the Managed Environment (e.g. VITA Rules, Agency-specific policies, applicable Federal regulations).

Iron Bow employees and any subcontractor partners will be required to attend Iron Bow's Security Awareness Training. Iron Bow will review these policies to ensure they meet or exceed the VITA Rules, Agency-specific

policies and applicable Federal Regulations. The training will provide Iron Bow employees with the information and tools needed to protect the confidentiality, integrity and availability of Iron Bow and Customer's information and information systems. It further ensures that all employees and contractors understand their information security responsibilities to protect such information and resources. Security Awareness Training is conducted upon hire and an annual, mandatory requirement, thereafter. Any mandatory VITA training will also be identified and completed.

6. Maintain administrative and System accounts in accordance with the SMM and VITA Rules.

Iron Bow will review their rules for maintaining administrative accounts to ensure they meet or exceed the SMM and VITA Rules. Tasks that Iron Bow will perform include, but are not limited to: creation and deletion of accounts and login credentials and passwords for those authorized access to such account; setting User permissions such as giving Users/restricting access to certain files; adding/deleting User Groups; and setting User Roles/Responsibilities to groups or individual Users. Administrative and System account information will be safeguarded in accordance with the SMM and VITA Rules.

7. Ensure that all Software and Hardware comply with authentication and security requirements in accordance with the SMM and VITA Rules.

Iron Bow will ensure the appropriate level of authentication is applied in accordance with the SMM and VITA Rules. Authentication methods include:

[redacted]

8. Ensure Environmental logs from all Devices are transmitted to the SIEM system in accordance with the SMM.

Iron Bow will send logged events on EUC supported devices to the MSS provide security tool. Iron Bow will request access to the security tool reports and read-only access to verify that logs are being sent successfully and being populated in dashboards and reports.

9. Coordinate efforts to ensure Security Management activities are kept up to date, managed effectively, have the appropriate tools and access, and are reported in accordance with the SMM and VITA Rules.

Iron Bow will utilize the MSS provided security tool to provide management and reporting in accordance with the SMM and VITA Rules.

Additionally, Iron Bow will coordinate with the MSI, VITA, Customers and other Towers with regard to Security Management activities. With the MSI and each Service Tower having a different focus from a scope and

infrastructure perspective, it will be important to communicate and jointly develop an enterprise security policy (or update the existing). Iron Bow will establish a security steering committee to further encourage a collaborative Environment. Operationally, Iron Bow will coordinate so that systems interface to push or pull data as may be required, enabling VITA and Customers to meet their business requirements. This will be done efficiently and securely to provide continuity of service to their constituents. From an incident/emergency perspective, Iron Bow will follow the procedure, as established in the SMM. Iron Bow will also comply with any cross-functional responsibilities and/or primary responsibilities laid out in the SMM. Iron Bow understands that reporting will be coordinated so that there is not duplication of efforts and Iron Bow will provide automation of such reporting to the greatest extent practicable.

10. Identify Security improvement opportunities and provide recommendations to MSI, MSS, and VITA in accordance with the SMM.

Iron Bow will work with the MSI, MSS, and VITA to identify security improvement opportunities and provide recommendations. Iron Bow will do this by performing their own security assessments. The security assessments will look at security posture and for ways to achieve a higher level of performance, and not simply meet minimum compliance. Iron Bow's assessments will categorize the findings as critical impact, high impact, medium impact or low impact. The assessments will also nominally provide feedback on identified strengths, as well as informational findings that are outside the scope of the assessments. Iron Bow will provide a list of actions to take to mitigate issues and to achieve a more ideal situation rather than simply satisfying a minimum requirement in a standard. Iron Bow will also access industry partners and subject matter experts in performing the assessment and in developing recommended solutions. Specific to security, Iron Bow's Practice Area Director meets with McAfee, Splunk, Tenable, Symantec, Cisco, Palo Alto, VMware, and EMC on a regular basis and has access to white papers, technical data, and demonstration gear, as well as access to OEM subject matter experts and will share information beneficial to VITA.

11. Establish and maintain mechanisms to safeguard against the unauthorized access, destruction, loss, or alteration of Customer data.

Iron Bow's personnel will help to safeguard against unauthorized access, destruction, loss, or alteration of customer data. Iron Bow's activities include but may not be limited to:

- Physical security and protection of the system console
- Maintain systems and servers – ensuring Patches are up-to-date
- Within the monitoring tools, whether at the system (server) or User (endpoint) level, set alerts
- Maintain system and servers with least number of packages possible. The more services and applications running, the greater the risk of opening the system to exploitation
- Monitor, maintain, and review system logs
- Maintain strict adherence to password policies, both system (Superuser password and any delegations) and User passwords
- Perform routine vulnerability scans to proactively detect irregularities
- Document system configurations and any changes, in accordance with Change Management policies

12. Provide, deploy, and maintain a solution to protect Devices that are directly connected to the Internet in accordance with the SMM and VITA Rules.

Iron Bow will use the MSS managed security tool and network based tools provided by the MSS to create a defined methodology for monitoring systems for unauthorized access, destruction, loss or alteration of Customers' data. Iron Bow will monitor reports and utilize read-only access to validate that Devices are meeting SMM and VITA Rules.

13. Perform and support security audits to check the effectiveness of the security procedures and controls in accordance with the SMM and VITA Rules.

Iron Bow will use the MSS provided security tools to protect, audit, and validate controls against VITA Rules. Iron Bow will use the MSS security tools to provide endpoint protection and will use McAfee product suite and [redacted] to audit and validate compliance with VITA Rules.

14. Initiate corrective actions in respect of any potential or actual security issues, risks, or noncompliance in accordance with the SMM and VITA Rules, and as directed by VITA or the MSI.

Audits or other analysis may uncover noncompliance/findings or identify risk which will result in a corrective action. In responding to corrective actions, Iron Bow will first understand the standard/control/policy which is being audited/violated and what constitutes compliance in order to build our corrective action plan. In determining the appropriate corrective action, Iron Bow will use root cause techniques such as Pareto Analysis or the 5 Why's to identify the true underlying issue. Working with resources from OEMs and corporate SMEs, and in coordination with VITA or the MSI (or other parties), Iron Bow will resolve the noncompliance and prevent reoccurrence.

15. Provide an audit status report detailing ongoing work and actions identified and completed in accordance with the SMM and VITA Rules.

Iron Bow support for audits will include providing status reports detailing ongoing work and actions identified and completed in accordance with the SMM and VITA Rules.

16. Implement, operate, and maintain the approved Cross-Service Tower solutions that meet all VITA's virus protection requirements in accordance with the SMM and VITA Rules.

Iron Bow will utilize the MSS provided security tools to deliver virus protection requirements. Iron Bow will use reports and read-only access to validate the requirements are being met.

17. Upon notification alert or acknowledgement of a malicious event, take immediate steps to asses and remediate in accordance with the SMM and VITA Rules.

One of the most critical components of responding to incidents is being prepared to respond before an incident occurs. Part of Iron Bow's preparation will be to ensure that there is a baseline of protection on all systems and networks in accordance with the SMM and VITA Rules. Iron Bow will ensure that written incident response procedures are developed and are widely available. Iron Bow will provide training on the procedures as well as conduct exercises to test our preparedness. The written procedures will also define who to contact and what steps must be taken should an incident occur. After identification, Iron Bow will obtain a full backup of the system in which suspicious events have been observed. Unless this evidence is immediately captured by making a full backup, it may be destroyed. The backup will also provide a basis for comparison to determine if future unauthorized activity occurs. Backup tapes will be safely stored so they will not be lost or stolen. Iron Bow will use a log book to record the nature of suspicious events observed immediately after they have been observed. Careful recording of these details will assist our efforts to identify the nature of an incident, develop effective solutions, and potentially prosecute those responsible. For Containment activities, Iron Bow staff will take measures to limit the scope and magnitude of the incident. As soon as Iron Bow recognizes that an incident has occurred or is occurring, our staff will immediately begin working to contain the incident. The first critical decision to be made during the containment stage is what to do with critical information and/or computing services. Iron Bow will work VITA to determine whether sensitive information should be left on information systems or whether it will be copied and taken off-line or moved to another system on another network where there is considerably less chance of interruption. The next decision concerns the operational status of the compromised system(s) itself. Iron Bow will work with VITA to determine if the system should be shut down entirely, disconnected from the network, or be allowed to continue to run in its normal operational status so

that any activity on the system can be monitored. Our recommendation to VITA will depend on the type and magnitude of the incident. If Iron Bow finds that the incident is being caused by a virus, it may be best to quickly eradicate the virus without shutting the infected system down. If the system is classified or sensitive, information or critical programs may be at risk, and it is generally best to shut the system down or to temporarily disconnect it from the network. If there is a reasonable chance that a perpetrator can be identified by letting a system continue to run as normal, risking some damage, disruption, or compromise of data may be advisable. Iron Bow will work with VITA to determine the most feasible and secure method of containment. During Recovery, Iron Bow will restore the system(s) to its normal operational status. In the case of relatively simple incidents such as attempted but unsuccessful intrusions into systems, recovery requires only assurance that the incident did not in any way affect system Software or data stored on the system. In the case of complex incidents, such as malicious code, recovery may require a complete restore operation from backups. In this case, Iron Bow will first determine the integrity of the backup. Once the restore has been performed, Iron Bow will verify that the restore operation was successful and that the system is back to its normal condition.

18. Recommend new Supplier Security Tools included as part of the Services (including any Equipment and Software products) that would reduce malware infection on Workstations or improve the cleanup of infections on Workstations and decrease the need for reimaging Workstations.

Iron Bow will provide VITA with a solution that focuses on endpoint detection and response (EDR). Furthermore, Iron Bow will partner with top security vendors that have focused on malware identification, response, and remediation as part of their offerings. With the rapid evolution of new capabilities, many vendors are providing increasing integration with other endpoint products as well as network security products. This has led to Security Orchestration, Automation, and Response (SOAR) which is rapidly gaining adoption. Iron Bow will provide access to road map information from their partner security vendors and compare the information to the vendor landscape to provide the best vendor agnostic recommendations to VITA.

19. In coordination with the MSI, leveraging new Supplier Security Tools that would improve VITA's business processes and performance.

Iron Bow will test and validate different vendor tools in their lab, ensuring the EUC Technicians have the required expertise to support new security tools. This will allow Iron Bow to provide expertise on any new tools and test integration with existing tools without affecting the VITA production Environment. By doing so, Iron Bow will provide for faster improvement of VITAs business processes and performance.

20. Maintain the technical and functional specifications and requirements for the Supplier Security Tools and any interfaces in accordance with the SMM and VITA Rules.

For SCCM, Cherwell Service Management and Cherwell Asset Management, Iron Bow will maintain the technical and functional specifications and requirements for the Supplier Security Tools and any interfaces in accordance with the SMM and VITA Rules.

21. Educate and train Supplier Personnel and support professionals in the use of Supplier Security Tools in accordance with the SMM and VITA Rules.

Prior to deploying any tool, Iron Bow will provide training to EUC Supplier Personnel and/support professionals as requested by VITA and the MSI. Iron Bow will bring OEM experts onsite to conduct the training if and when it is available from the OEM. Training will be extended to other personnel in the enterprise as needed.

22. Provide role-based access to monitoring and reporting interfaces for the VITA Security Tools.

Iron Bow will leverage VITA MSS security tools to monitor and report on Iron Bow supported computers. Iron Bow will work with MSS to define appropriate role-based access control.

23. Provide access to a raw feed as well as to monitoring and reporting interfaces for the Supplier Security Tools dedicated to VITA in accordance with the SMM and VITA Rules.

Iron Bow will utilize the VITA MSS security tools to the furthest extent possible to provide the most effective means of complying with VITA Rules and provide immediate access to relevant log files. Where this is not possible, Iron Bow will provide access to logs associated with Iron Bow security tools.

24. Use VITA and MSS provided or approved tools to diagnose and resolve Security/Malware/Spyware/Virus incidents.

Iron Bow has expertise working with a large set of tools, which includes tools for diagnosing and resolving incidents. Iron Bow will utilize this expertise to address incidents using VITA and MSS provided tools. Iron Bow will provide value added support by recommending additional levels of orchestration and automation. Iron Bow will work with VITA to obtain access to reports and read only access to use VITA and MSS provided tools to diagnose incidents.

25. Provide Support for all Incidents related to virus, malware or spyware and work with VITA, MSI, and MSS in the event of a potential security risk or breach, virus, malware or spyware outbreak to collect, disseminate, and report data from potentially compromised systems in accordance with the SMM and VITA Rules.

Following the process outlined in Section 2.5 #17 above, Iron Bow will support all incidents related to virus, malware or spyware and work with VITA, MSI, and MSS in the event of a potential security risk or breach, virus, malware or spyware outbreak to collect, disseminate, and report data from potentially compromised systems in accordance with the SMM and VITA Rules.

26. Partner with VITA, MSS, and MSI to test new security tools and updated versions and report and provide feedback on the effectiveness of each new security tool in accordance with the SMM and VITA Rules.

Iron Bow will partner with VITA, MSS, and MSI to test new security tools and updated versions of such tools. Iron Bow will bring tools into the corporate lab in Herndon, Virginia to test. Because of OEM relationships, Iron Bow will leverage white papers and benchmarking data from the OEMs that would otherwise not be available. Any data or results of such testing will be shared with the MSI, MSS, and/or VITA.

27. Notify VITA, the MSI, Customers, or other suppliers of any health check, internal assessment, or internal security audit violations in accordance with the SMM.

Iron Bow will utilize MSS security tools to validate compliance and will notify VITA, the MSI, Customers, and/or other suppliers if issues are found using the reports and read-only access provided to the MSS security tools. With this access, Iron Bow's security team will follow a schedule for conducting health checks or other internal assessments in addition to the automated scanning/reporting built into the system. Results of any violations will be shared across the enterprise.

28. Identify internal security violations, including Enterprise Security policies, and remediate risks that are identified in accordance with the SMM and VITA Rules.

Iron Bow will report any violations that are identified. Upon identification, Iron Bow will first look to contain (as needed) and assess risk to Users, systems, VITA, the MSI, or other Service Towers- The risk assessment will include determining how many systems or Users have been potentially impacted as well as whether or not information been compromised. Risks will be logged and tracked on a risk register until remediated or otherwise mitigated.

29. Develop and implement remediation plans for security audit and assessment findings in accordance with the SMM and VITA Rules. Remediation of Supplier non-compliance and deficiencies will be completed at Supplier's expense.

Iron Bow will develop an information security remediation plan which outlines all of the findings, as well as defines the approach for fixing the security related issues. The remediation plan will describe how risks are identified, the action taken to decrease exposure to a larger group of Users, the steps taken to correct the issues/address the findings, the precautions taken to prevent the issue from spreading or reoccurring, and the plan to validate and verify that the actions taken have successfully remediated the risk or issue thereby ensuring the right processes and controls are place. Remediation of Iron Bow non-compliance and deficiencies will be completed at Iron Bow's expense.

30. Coordinate audit related activities for in-scope functions in accordance with the SMM and VITA Rules.

Any activities related to audits in Iron Bow's AOR will be coordinated in accordance with the SMM and VITA Rules.

31. Make reports available to VITA for evaluation of remediation plans and results in accordance with the SMM and VITA Rules.

Iron Bow will provide remediation plans and/or any reports specific to remediation efforts for evaluation and review, as needed.

32. Maintain all security documentation related to VITA's enterprise security architecture for Equipment, Software, and Networks in accordance with the SMM and VITA Rules.

Iron Bow will provide the required level of documentation. This may include but not be limited to systems architecture diagrams, security plans, test plans, or other documentation.

33. Monitor and manage activities to ensure Security Software is installed on Devices connected to the VITA network.

Iron Bow will utilize the MSS provided security tools to the fullest extent possible. Iron Bow will monitor and manage activities using reports and read-only access provided by MSS to their security tools and/or infrastructure. Iron Bow will ensure that the Security Software is installed on all Devices Iron Bow provides and/or supports.

34. Provide ongoing feedback to improve various security Software and monitoring tools, ensuring products are running efficiently.

Iron Bow will provide VITA with a solution that focuses on endpoint detection and response (EDR). Furthermore, Iron Bow will partner with top security vendors that have focused on malware identification, response, and remediation as part of their offerings. With the rapid evolution of new capabilities, many vendors are providing increasing integration with other endpoint products as well as network security products. This has led to Security Orchestration, Automation, and Response (SOAR) which is rapidly gaining adoption. Iron Bow will provide access to road map information from their partner security vendors and compare the information to the vendor landscape to provide the best vendor agnostic recommendations to VITA.

35. Install, update and maintain Malware Protection Software and systems in accordance with the VITA security requirements for all Software and Equipment in the VITA Environment.

Iron Bow will utilize the MSS managed security tools to the fullest extent possible. Iron Bow will monitor and manage activities using reports and read-only access provided by MSS security tools and/or infrastructure. Iron Bow will ensure that the Malware Protection Software is installed on all Devices Iron Bow provides and/or supports.

36. Respond to Malware infections in accordance with the SMM and VITA Rules.

Iron Bow will respond to Malware infections in accordance with the SMM and VITA Rules and in the event systems become infected with malware, Iron Bow will minimally provide the follow services:

1. Identify and isolate the affected systems
2. Patch vulnerabilities and ensure Environmental compliance
3. [redacted]
4. Confirm that the recommended best practices are in place
5. [redacted]
6. Run a full On-Demand Scan on all systems
7. Confirm control of the Environment
8. Place the isolated systems back online once they are confirmed clean
9. Restore the affected files from a backup
10. Perform incident response and proactive measures
11. Consider implementing additional recommendations

2.5.1 Security Incident Response, Planning and Investigation

1. Respond to Security Incidents in accordance with the SMM and VITA Rules.

Iron Bow will provide a coordinated response to any security incidents in accordance with SMM and VITA Rules. Iron Bow will respond to security incidents in accordance with the established Incident Response Plan included in the in SMM and maintained in the MSI's Document Repository. Within each phase of the Incident Response Plan, there are specific areas where Iron Bow's EUC Technicians will provide support as needed: 1) Preparation; 2) Identification; 3) Containment; 4) Eradication; 5) Recovery; and 6) Lessons Learned.

All members of Iron Bow's EUC staff will be trained and understand what to do in the event of an incident. Every Team member will review the Incidence Response Plan in detail and the plan will be easily accessible to ensure that when an incident does occur, the right procedures are followed. Iron Bow will also practice response to incidents.

Iron Bow will perform activities including but are not limited to: making an initial assessment; communicating the incident; containing the damage and minimizing the risk; identifying the type and severity of the compromise; protecting the evidence; recovering systems; compiling and organizing incident documentation; assessing incident damage and cost; and review the response and updating policies.

2. Provide, as requested by VITA, the MSI, Customers, or other suppliers, any logs or alert/events information to assist in responding to Security Incidents in accordance with the SMM and VITA Rules.

As requested by VITA, the MSI, Customers, and/or other suppliers, Iron Bow will provide any information needed in responding to Security Incidents in accordance with the SMM and VITA Rules.

Our activities will include, but not be limited to:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- Review intrusion detection system logs for [redacted]

- Examine other log files for [redacted]
- Compare systems to previously conducted file/system integrity checks.
- Search for sensitive data, such as credit card numbers and employee or customer data, which may have been moved or hidden for future retrieval or modifications.
- Match the performance of suspected systems against their baseline performance levels.

3. Provide immediate on-demand automated electronic Software deployment solution for Security Incidents detection, remediation, and prevention efforts in accordance with the SMM and VITA Rules.

Iron Bow's overall solution includes tools which emphasize integration, automation, and orchestration as the foundation of the threat defense lifecycle. Through harnessing the power of machine learning to detect zero-day threats in near real time, these tools streamline Iron Bow's ability to quickly expose and remediate advanced attacks so security and productivity are not compromised. These tools are centrally managed using a single pane of glass and defend against the full threat spectrum from zero-day exploits to advanced targeted attacks, protecting Windows, Macs, and Linux systems. Our solution is described in section 2.5, Security, above.

4. Monitor for and resolve suspicious activity or patterns that may be indicative of an End User Device issue requiring Resolution (e.g., virus, rogue application).

Iron Bow will monitor dashboards and reports from the MSS managed security tools to identify suspicious activity. Iron Bow will also take advantage of any additional access provided to the MSS vulnerability assessment tools and other network monitoring tools to identify suspicious activity. Iron Bow will work with the other teams to provide as much automated remediation as possible. Additionally, Iron Bow will work with VITA to recommend tools or additional programming that will orchestrate and automate the remediation process where applicable. Iron Bow will prioritize remediation and remediate systems as quickly as possible.

Iron Bow will provide security SMEs that are experienced in supporting common security data sources including network security, endpoint solutions, malware and payload analysis, network and wire data, identity and asset management systems, and threat intelligence, which will accelerate deployment and adoption for VITA.

5. Provide support to security team to identify and collect Hardware affected by any security event.

At the direction of the security team, Iron Bow will identify and gather Hardware affected by the security event. This may include, but not be limited to, determining the attack point of origin and intent of the attack, as well as identifying the systems that have been compromised and files that have been accessed.

6. Make Supplier Personnel available for interviews by VITA incident response teams.

All Iron Bow personnel will be available for interviews by any incident response team.

2.5.2 Security Configuration Compliance

1. Comply, implement, document, and enforce Device configurations in accordance with the SMM and VITA Rules.

Iron Bow will comply, implement, and enforce Device configurations in accordance with the SMM and VITA Rules. Configurations will be established by groups using group policy object (GPO) and applied to End User Devices. Security policy is established by VITA and Iron Bow understands the policy is applied and enforced by the MSS. Iron Bow will assist the MSS to the greatest extent allowable in the application and enforcement of compliance through the MSS provided Security tools.

2. Provide automated detection and enforcement of VITA critical security components, configuration settings, and Patch policies in accordance with the SMM and VITA Rules.

Iron Bow will use the MSS provided security tools to automate security audit processes and ensure reporting is consistent and accurate against internal and external policies to the greatest extent allowable. Iron Bow will perform audits across both managed (agent-based) and unmanaged (agentless) systems and unify management of policy audits and endpoint security through the use of the MSS provided Security tools.

3. Detect, in accordance with the SMM and VITA Rules, when previously applied policies are no longer in effect and reapply those policies.

Iron Bow will use the MSS provided security tools to access the up-to-date data, dashboards and reports and to detect when previously applied policies are no longer in effect. Iron Bow will collaborate with the MSI, MSS provider and VITA to resolve such issues.

3.0 EUS

3.1 Initial Operating Capability

1. Assume the ownership, operation, management, and maintenance of all Incumbent Supplier-provided End User Computing services.

Iron Bow understands that "Initial Operating Capability" includes all of the activities associated with the analysis, planning, and execution of the transfer of all current EUC services from the incumbent. Iron Bow will ensure a seamless transfer on the Commencement Date that will not be disruptive to Customers. Iron Bow's plans for service takeover, transition, and commencement of services will be detailed in the Implementation Plan.

2. Assume responsibility for completing all existing IMACs, projects, and work orders open as of, or scheduled beyond, the Commencement Date in accordance with the committed schedule.

Iron Bow will re-badge all those incumbent personnel who are performing well in support of VITA. This will make it easier for Iron Bow to provide both continuity of service while retaining critical corporate knowledge. Iron Bow expects that VITA, in coordination with the incumbent, will provide Iron Bow the most currently available list of IMACs, projects, and open work orders that must be completed. Iron Bow, to include the incumbent personnel, will work with VITA to review and prioritize the list prior to commencing work. This is critical step within the Implementation process. Iron Bow will ensure all projects and work orders are documented and therefore tracked within Cherwell.

3. Refresh existing End User Devices per their currently scheduled refresh date (e.g., do not pause refreshes for 30 days, or re-baseline refresh windows based on the Commencement Date).

Iron Bow will refresh End User Devices according the Annual Refresh and Currency Plan. Agencies delaying approval refresh of existing machines until the new EUC Supplier is announced may increase the number of refresh eligible Devices significantly. Iron Bow will provide a plan to manage high number of refresh approvals shortly after Commencement Date and also note this concern in the Risk Register.

4. Support all existing End User Devices, Software, and service configurations currently performed by or contracted with Incumbent.

Iron Bow will support all existing End User Devices, Software, and Services configurations which were performed by the incumbent. Through Implementation and after Commencement, Iron Bow will review existing processes and establish standard operating procedures. In collaboration with VITA, the MSI, and the other Service Towers, Iron Bow will ensure continuity of service at Commencement while continuously seeking to evolve services and technology.

5. Support all VITA and Customer Sites and hours of operation currently supported by Incumbent.

Iron Bow will support all VITA and Customer Sites and hours of operation currently supported by the incumbent. Iron Bow has included RUs for alternate hours of services include 24x7 and VIP coverage.

6. Develop and publish FAQs, wikis, and other self-help documentation to guide Users on the installation of clients in coordination with MSI.

Iron Bow will develop and publish FAQs, wikis, and other self-help documentation to guide Users on the installation of clients, as well as other forms of training within Cherwell Knowledge Management (as integrated with the SMS). This includes the development and publication of knowledge articles, and logging known errors in the Known Error Database through the MSI Portal.

3.2 Additional Required Services

"Additional Required Services" includes services that do not exist today but that the Commonwealth plans to acquire under this contract. Iron Bow has priced these separately from the standard offerings.

3.2.1 Device Backup

1. Provide End User Device-level and Mobile Device-level backup/recovery solution, to include:

Iron Bow will provide for, if purchased by VITA under this contract, on-premise End User Device level backup ([redacted] solution for Windows Devices. Our solution employs variable-length deduplication, which significantly reduces backup time by only storing unique daily changes while maintaining daily full backups for immediate, single-step restore. Iron Bow will scale to meet the needs of exponential data growth, regulatory compliance, increased SLAs, and shrinking backup windows. The [redacted] solution will allow Iron Bow to provide flexible deployment options for fast, daily full backups.

This solution delivers efficient data protection for desktop/laptop by providing data deduplication, open-file backup, and CPU throttling. [redacted] leverages existing network links, and since it operates in the background, it is not disruptive to end-users. Data is automatically backed up when a User is attached to the network during normal backup windows. [redacted] enables self-service backup and recovery where End Users can initiate an on-demand backup and quickly recover their own data anywhere, anytime, via an intuitive interface and integrated search engine in just one-step.

For non-Windows Devices, Iron Bow will provide for, if purchased by VITA under this contract, a cloud-based mobile Device-level backup/recovery solution [redacted] provides a next generation backup, restoration and archival solution enabling point and click disaster recovery and data loss prevention. With enterprise grade encryption in-transit (256-bit TLS) and at-rest (AES 256-bit), [redacted] offers the highest level of data security and privacy, meeting or exceeding all of the Commonwealth's security requirements detailed in the VITA Rules.

3.2.2 Enterprise Mobility Management

1. Configure mobile Devices (e.g., iOS or Android) to include installing VPN application, Mobile Device Management (MDM) client, specific applications, and provide access to Commonwealth services (e.g., messaging).

Iron Bow will provide for an MDM solution if purchased by VITA under this contract. Iron Bow will use the MDM solution to configure Devices during initial power on with bulk provisioning programs such as the Apple Device Enrollment Program (DEP) and Windows Out-of-Box Enrollment (OOBE). Iron Bow will deploy public, internal or bulk-purchased apps to Devices automatically or to an enterprise app catalog for on-demand install. The MDM solution will allow Iron Bow to self-activate Devices by entering their corporate credentials in a simple MDM onboarding workflow. Iron Bow will connect End Users to enterprise email, VPN, Wi-Fi, content, intranet sites

and other backend resources, while configuring MDM policies for Device restrictions, layout, settings access, notifications and assign based on OS or ownership type (BYOD or Commonwealth-owned).

2. Provide assistance with Mobile Device Management (MDM) application installation, configuration, updating, and incident resolution.

Iron Bow's Field Service Technicians will provide mobile device management support to include, but not be limited to providing daily review and resolution of incidents and work orders, and other services to End Users. Incidents and work orders may include performing preventative maintenance, resolving issues relating to Software and equipment problems to address mobile device service needs. Iron Bow will ensure no service is performed that invalidates the warranty of the Device. Iron Bow will coordinate with the OEM to provide warranty support as needed.

3. Support mobile Devices that are Commonwealth-owned.

Iron Bow will provide support on mobile Devices that are Commonwealth-owned as a Solution Request (Project).

4. Support VITA-approved mobile Device OS including iOS and Android.

Iron Bow will support VITA approved mobile Device OS, including iOS and Android using [redacted].

5. Support all standard Software, in accordance with the SMM, in a mobile Environment.

[redacted] supports all standard Software, which includes updating Software on the Device and monitoring mobile Device health and providing troubleshooting assistance. Iron Bow will provide maintenance, such as Patches and updates, as well as troubleshooting Customer issues with Hardware or Software.

6. Provide end-to-end diagnostic of mobile Device, Software, and connectivity faults.

Iron Bow's Field Service Technicians will have access to a variety of diagnostic tools to troubleshoot mobile Devices, Software and connectivity faults and will provide end-to-end diagnostic mobile Device, Software and connectivity faults.

7. Manage mobile Device compliance in accordance with the SMM and VITA Rules.

Iron Bow will protect information through Device security and data loss prevention (DLP) policies which will comply with the SMM and VITA Rules, as well as enabling Device-level encryption, data encryption and Hardware security policies (TPM, biometrics, etc.). The Mobile Device Management (MDM) solution provides Iron Bow with the ability to: prevent data loss with app sharing permissions, copy/paste restrictions, and geo-fencing policies; monitor for malware threats or jailbroken Devices and automatically remediate with a remote lock, Device wipe or customizable Device quarantine controls; and configure policies including: app blacklists, Device pairing, Wi-Fi security, and TLS enforcement.

8. Manage the Mobile Device Management (MDM) Tool in accordance with the SMM and VITA Rules.

Iron Bow will manage the MDM tool in accordance with the SMM and VITA Rules.

9. Develop and publish FAQs, wikis, and other self-help documentation to guide Users on the installation of clients in coordination with MSI.

Iron Bow will develop and publish FAQs, wikis, and other self-help documentation to guide Users on the installation of clients, as well as other forms of training within Cherwell Knowledge Management (as integrated with the SMS). This includes the development and publication of knowledge articles, and logging known errors in the Known Error Database through the MSI Portal.

10. Ensure that mobile Devices are Patched and upgraded in accordance with the SMM and VITA Rules.

Iron Bow will ensure that mobile Devices are Patched and upgraded in accordance with the SMM and VITA Rules. See 3.2.2 #5 above.

11. Provide end-to-end support for mobile Devices for Users, including:

11.1 Mobile Device setup / configuration.

11.2 Install mobile Device support Software.

11.3 Provide brief orientation to Users regarding their new Device and support options.

Iron Bow will provide [redacted] for end-to-end support for mobile devices for Users including mobile device set up/configuration and software installation. Iron Bow will provide an orientation for Users covering the new Device and support services.

4.0 Enhanced Services

Enhanced Services includes services that do not exist today but that the Commonwealth may opt to acquire in the under this contract. Iron Bow has priced these separately from the standard offerings.

4.1 Application Virtualization

1. Produce application virtualization packages of many different configurations.

Iron Bow will utilize [redacted] to virtualize applications. The process begins by first assessing the viability of each application in a virtualized setting. Iron Bow will then set up a new virtual machine (VM). Assuming the goal is to use the virtual application in a VDI Environment, most administrators configure this VM to mimic one of their organization's virtual desktops, rather than using an actual production virtual desktop. Once Iron Bow has configured the virtual desktop, the next step is to take a VM-level snapshot. If Iron Bow creates the snapshot while the VM is running, then memory does not have to be captured within the snapshot. After the snapshot is created , Iron Bow will log into the VM and run the [redacted] utility. This utility performs a pre-scan of the VM, which documents the VM's contents (system files, registry entries and more) before Iron Bow installs the application to be virtualized. When creating application virtualization packages, Iron Bow will ask VITA for their requirements on miscellaneous items such as whether a separate DAT file, .MSI package and/or compressed package is required. Once the requirements are provided, Iron Bow will create the package.

2. Ensure packages containing one or more applications to be virtualized operate properly inside the virtualized Environment.

See Section 4.1 #1 above.

3. Include registry virtualization that allows for isolation that is configurable down to individual registry values.

[redacted] defines application virtualization as the ability to deploy Software without modifying the host computer or making any changes to the local OS, file system, or registry.

Central to [redacted] is application isolation, which enables Software delivery without changes to the file system and registry of the host computer. [redacted] not only allows previously incompatible versions of the same application to be co-located, but also allows them to run side-by-side. Other applications running on the same PC will not be aware of virtualized applications, so regression testing—a major cost of application deployment—is reduced dramatically. [redacted] file system and registry isolation prevent applications from being affected by other Software installed on the same system. Two versions of the same application can appear to be installed and run from the same directory without conflict, even where virtual and non-virtual versions exist at the same

location. [redacted] also provides Windows side-by-side DLL isolation without having to redevelop applications or upgrade to another version of Windows.

4. Produce a package that will run without any administrative privileges.

Because [redacted] requires no Device drivers, it will run applications without administrator rights and requires zero changes to the PC—even if the End User is running on a locked-down PC. Single application packages are supported by any Windows platform. Virtualized applications will run without requiring any modification of administrative security permissions, which protects the host OS from possibly corruptive installation modifications.

5. Produce a package that does not require a formal installation to successfully run on the host server.

[redacted] accomplishes its zero footprint, agentless installation by embedding its entire runtime into each packaged executable. Because the runtime is very small (~400KB) and package data is stored in a compressed state, the overall disk footprint is usually two times smaller than traditional deployments of the same application without [redacted].

6. When required, produce a package that can successfully run on non-VITA Devices.

[redacted] will easily convert standard applications like Microsoft Office into portable applications that can run from USB flash drives or CD-ROM. For USB deployments, [redacted] portable mode redirects application registry and file system changes intended for the host PC to files stored on the portable Device. Because [redacted] has no Device drivers and runs in Guest/Restricted User accounts, [redacted] portable applications will be used on kiosk PCs, even if they are locked down and do not permit any installation.

7. Produce a virtualized application that, when executed, is isolated by default from all other applications executing on the same computer.

See Section 4.1 #3 above.

8. When required, virtualized applications can be selectively exposed to the underlying OS to allow for interaction between the virtualized application and non-virtualized applications.

The impact of deploying virtualized applications is the same as deploying any normal application. In a Windows Environment, the EXEs generated by [redacted] are simple, notepad-like applications that run without external dependencies. Deploying agentless virtualized applications does not affect other applications on the system.

4.2 Virtual Desktops Operations

Iron Bow's methodology to provide virtual desktop operations will focuses on five key areas:

- Assess: Assess current state relative to a validated design, identify gaps and remediation
- Design: Create a remediation plan to close the gap between current and proven solution state
- Deploy: Implement or remediate against the proven solution and integrate that into your ecosystem
- Knowledge Transfer: Operationalize the solution in the client Environment. Focus on running and supporting the solution
- Validate: Validate complete solution from technology, people, and process prospective

Iron Bow will provide in depth analysis to determine virtualization paths for development and deployment. Focusing on best practice methodologies, Iron Bow generates and provides an infrastructure baseline. The baseline identifies CPU, memory, bandwidth and storage consumption. In doing so, Iron Bow is able to identify application consumption and constraints. The long term outcome is a closer alignment with application consumption and the End Users leveraging identified applications. The design portion begins with identifying an

overall management schema acceptable to VITA. Iron Bow recommends a 3-Tiered Virtualization approach: 1) Cluster Design; 2) Storage Design; and 3) Network Design.

1. Provide Virtual Desktop Infrastructure services (VDI).

The virtualization of the desktop component requires an in-depth analysis of the current applications being consumed on existing desktops. Iron Bow uses an assessment methodology for determining which Users make strong candidates and which ones should be avoided. There will be approximately 10-20 percent of Users that do not make strong candidates for a virtualized desktop, primarily due to bandwidth restrictions and expensive Hardware costs in supporting their required applications. Iron Bow's assessment of the client infrastructure identifies those constraints and the cost structure of whether an individual receives a virtualized desktop or continues their physical desktop use.

Iron Bow will leverage [redacted] and MS (Gold) Partnership for Devices and deployment. Iron Bow will leverage certified professionals in our delivery organization to assist Iron Bow on-site staff with these tasks. [redacted] is Iron Bow's platform of choice to transform static desktops into secure, digital workspaces. It will allow Iron Bow to provision virtual or remote desktops and applications through a single VDI and app virtualization platform to streamline management and easily entitle End Users.

Iron Bow has provided an RU which includes the Labor, Software, Consulting and Monthly Recurring Facility Costs required to manage and maintain the delivery of a VDI solution. Since infrastructure costs differ dramatically depending on the size of the solution (i.e. small agency vs. large agency (over 2,000 users), the infrastructure costs are not included at this time. If VITA is interested in deploying VDI, Iron Bow will work with VITA to determine the appropriately sized infrastructure.

2. Perform the Configuration of settings within the VDI platform.

Using [redacted], Iron Bow will configure [redacted], create administrators, provision and deploy [redacted], set up User authentication, configure policies, and manage [redacted] applications in [redacted]. When configuring [redacted], Iron Bow will set security policies, as well as integrate any other services or tools. Iron Bow will create one virtual machine as a base image, and use [redacted] to generate a pool of virtual desktops from that image. Iron Bow will then install or stream applications/application packages to pools of desktops with [redacted]. Pools can be one, hundreds, or thousands of desktops. [redacted] allows applications/application packages to be tied to specific AD groups to establish permissions – which are tied to pools of desktops. Users can view the desktop view once entitled. Users will be added and removed from AD groups from a central location without modifying or updating individual packages that were deployed previously.

3. Configure and support VDI services on End User Devices.

In [redacted], Iron Bow manages desktop pools, virtual-machine desktops, and desktop sessions. Administration and services Iron Bow provides are simplified in a virtual Environment since it is being performed in a central location.

4. Define, in collaboration with VITA, the Operating Systems, Software, and encryption / security functionality, etc. that will be incorporated into the core images, and update the image definitions as directed.

Iron Bow will define and work in collaboration with VITA to define the VDI Environment and will recommend changes to the core images based upon Enterprise growth and evolution of technologies. Iron Bow will continue to leverage MDT and SCCM to assist in image building and delivering Patches. Iron Bow will develop, design, engineer, test, and document processes for provisioning and subsequent maintenance of server Software in support of the VITA secure standard Image. Iron Bow will use the VITA-defined baseline image in all image builds for the various Hardware platforms and install all approved 3rd party Software (e.g., MS Office Future Releases,

Adobe Applications and Future Releases, Anti-Virus Application and Future Releases, Patch Management, Non-Baseline SW Installs, and Third-Party Plug-Ins).

5. Create a set of core images or core image profiles based on VITA-defined requirements for use on virtual desktops.

Iron Bow will support the VITA baseline image by installing images using SCCM; securing virtual machines; installing and/or updating Device driver(s); and maintaining Patches. Iron Bow will create or update operation and maintenance documentation for all Hardware and Software.

Iron Bow will leverage SCCM and VDI as part of the image upgrade process. The process involves testing the upgrades against a small subset of known good images, identifying any updates that negatively impact User capabilities, identifying mitigation strategy against not using those updates and updating the image for deployment. Utilizing VDI allows Iron Bow to create new desktop pools and images and entitle to Users, while maintaining old image for failback measures should an impact be identified.

End point management is an integral part of any VDI deployment and Iron Bow will do so in accordance with the VITA Rules and the requirements described herein. . All these services are built into the Windows image that will support the VDI infrastructure at the time of image creation by the Team.

6. Update and retest each core image as new versions of Software are made available.

See Section 4.2 #5 directly above.

7. Collaborate with the MSI to develop the self-service instructions for the deployment of client tools to End User Devices.

Iron Bow will collaborate with the MSI to develop the self-service instructions for the deployment of client tools to End User Devices. As stated previously, Iron Bow will build an interface with the MSI's Knowledge Management System so that any Knowledge articles, FAQs, wikis or other self-help/self-service documentation or instructions created in Iron Bow's system will seamlessly transfer to the SMS.

8. Review and as appropriate recommend the application(s) to be deployed for the virtual desktop platform.

See Section 4.2 #1 above.

4.3 Operating System Virtualization

1. Provide a virtualized desktop-based Operating System Environment for designated Users in which to run legacy applications.

[redacted] will support multiple, concurrent running copies of an application on the same PC. [redacted] supports multiple, concurrent application versions to support VITA's production release cycle. [redacted] will allow VITA to take advantage of new features immediately without affecting previously deployed applications.

2. Provide a solution that does not require any servers, databases or other infrastructure (i.e., runs entirely on the End User Device).

The virtualization that will be provided by Iron Bow uses Software to simulate the existence of Hardware and create a virtual computer system. Doing this allows businesses to run more than one virtual system – and multiple OS and applications -- on a single desktop device. Each self-contained VM is completely independent. Putting multiple VMs on a single computer enables several OS and applications to run on just one physical server, or host. A thin layer of Software called a hypervisor decouples the virtual machines from the host and dynamically allocates computing resources to each VM as needed.

3. Provide capability to allow Users to access Hardware ports (e.g., USB) attached to the physical host directly from the virtual desktop Operating System.

[redacted] easily converts standard applications like Microsoft Office into portable applications that run from USB flash drives or CD-ROM. For USB deployments, [redacted] redirects application registry and file system changes intended for the host PC to files stored on the portable Device. Because [redacted] has no Device drivers and runs in guest/restricted User accounts, [redacted] portable applications are used on kiosk PCs, even if they are locked down and do not permit any installation.

4. Deploy a virtual desktop Operating System image built from the standard End User Device imaging process which includes all minimum Software applications, clients and settings.

See Section 4.1 # 4 and #5 above.

4.4 Value Added Services

1. Provide additional services and offerings that may enhance the Commonwealth's End-User Services.

Iron Bow can provide the following services:

- For Agencies that may have high privacy requirements that restrict using a public cloud, the [redacted] is an on-premises, air-gapped option.
- Serve as clearing house for major COTS vendors and applications to enable the Commonwealth to better leverage buying power and lower per seat cost across all agencies. Central license and media management will allow for quicker Software deployment, and supports new license approval workflows.
- Cyber-security consultations: Our advanced Cyber Security SMEs are available to support the Security STS, MSI, and VITA on project-based initiatives. Our expertise includes: Policy Enforcement, Network Defense, Network Vulnerability Assessment, Threat Visibility, and Remediation and Response.
- Hosted and Managed Voice Solution
- Wireless and Network Troubleshooting, Consulting and Support
- Secure Transport or relocation of Servers at a per Device cost
- Destruction of Network Printer Hard Drives, at the request of the Managed Print Provider
- HP Tech Café Market Services

  The HP Tech Café Market vending machine provides End Users with instant, self-service access to the IT accessories and supplies they need. In less than a minute, at any time of day, End Users can visit this self-service machine to obtain a variety of different accessories including keyboards, batteries, mice, power supply adapters, and more. Integrated approval, billing, and inventory fulfillment will increase productivity of End Users. Iron Bow has the ability to choose which products to offer and how often they are accessed, tracking the peripherals being obtained through employee badge identification.
  - HP Tech Café Market locker instead of, or in addition to, the vending machine for a safe storage place that allows employees to procure larger Devices or send them out for repair or replacement.

4.4.1 Centralized Asset Disposal for all Service Tower Suppliers

Iron Bow will provide Centralized Asset Disposal for all STS's. The STS will submit a Service Request through the SMS for Asset Disposal - Other than EUC. Iron Bow will review the Service Request with the STS to determine if the request will be handled as a Service Request or as a Project (depending on the size and complexity of the disposal request). Each Device will have a cost for disposal. For Service Requests that are re-classified as a

Project, Iron Bow will provide a proposal with an estimated cost, assigned resources, and schedule. SLAs will be agreed to with the STS requesting the Service.

Service	Service Description	Charged Per	Desktop and Laptop	Monitors (LCD)	Phone	Networking	Servers	Printer /Copier (Rolling)	Printer (Table Top)
Storage and Delivery	End of Life IT Assets will be Stored at one of Core Technologies Depots. Accumulated COV assets will be transported to a DGS facility as needed.	Delivery	$ 125.00	$ 125.00	$ 125.00	$ 125.00	$ 125.00	$ 125.00	$ 125.00
Trip Charge	One time fee per location, unlimited quantity of assets	Stop	$ 50.00	$ 50.00	$ 50.00	$ 50.00	$ 50.00	$ 100.00	$ 50.00
Mileage	Mileage will be charged to and from a location. Pick up Routes will be combined when ever possible to reduce Mileage charges	Mile	$ 0.53	$ 0.53	$ 0.53	$ 0.53	$ 0.53	$ 0.53	$ 0.53
Tech Time	Level One technician	Hour	$ 40.00	$ 40.00	$ 40.00	$ 40.00	$ 40.00	$ 40.00	$ 40.00
Labor/Packing	Labor to Pack, Palletize Equipment. Includes all Supplies	Hour	$ 30.00	$ 30.00	$ 30.00	$ 30.00	$ 30.00	$ 30.00	$ 30.00
Asset Disposal	Asset Tracking and Reporting, Data Destruction, Recycling Services	Asset	$ 10.00	$ 20.00	$ 10.00	$ 10.00	$ 15.00	$ 15.00	$ 15.00
Redeployment Services	Asset Tracking and Reporting, Data Destruction if required and delivery to Holding Depot	Asset	$ 15.00	$ 15.00	$ 15.00	$ 15.00	$ 75.00	$ 75.00	$ 50.00
Mail Back Program	Pre-labeled shipping box will be provided for customer to return assets. Asset Tracking and Reporting, Data Destruction and Recycling Services	Asset	$ 20.00	$ 20.00	$ 20.00	$ 20.00	$ -	$ -	$ -
No Show		Ticket	$ 50.00	$ 50.00	$ 50.00	$ 50.00	$ 50.00	$ 50.00	$ 50.00
Hard Drive Destruction, On-site	Hard Drive Piercing Services	Hour	$ 50.00	$ -	$ -	$ 50.00	$ 50.00	$ 50.00	$ 50.00
Hard Drive Destruction, Off-site	Hard Drive Piercing Services	Hour	$ 35.00	$ -	$ -	$ 35.00	$ 35.00	$ 35.00	$ 35.00
STS Storage Charge	Monthly charge to store a pallet of assets.	Month	$ 50.00	$ 50.00	$ 50.00	$ 50.00	$ 50.00	$ 50.00	$ 50.00

Figure 3 Asset Disposal Price List by Device

Sample Asset Disposal Scenarios:	Cost	Quantity	Extended
Department of Transportation			
Ticket Request notes to pick up 5 Copier/Printers in Richmond			
Applicable Charges would be:			
Trip Charge	$ 100.00	1	$ 100.00
Mileage (with in 25 mile radius)	$ -		$ -
Asset Disposal	$ 15.00	5	$ 75.00
Labor/Packing	$ 30.00	1	$ 30.00
Total			**$ 205.00**
Department of Motor Vehicles			
Ticket Request notes to ship back Three phones located in Bristol for Disposal			
Applicable Charges would be:			
Mail Back Program	$ 20.00	1	$ 20.00
Asset Disposal	$ 10.00	3	$ 30.00
Labor/Packing	$ 30.00	1	$ 30.00
Total			**$ 80.00**
Route Combined to Save Mileage Charges			
#1 Tax Department			
Ticket Request notes to pick up 10 Servers in Culpeper			
Applicable Charges would be:			
Trip Charge	$ 50.00	1	$ 50.00
Mileage: 95 miles Billed. Saves 95 miles	$ 0.53	95	$ 50.35
Hard Drive Data Destruction	$ 50.00	1	$ 50.00
Asset Disposal	$ 15.00	10	$ 150.00
Labor/Packing	$ 30.00	1	$ 30.00
Total			**$ 330.35**
#2 Department of Blind and Visually Impaired			
Additional Ticket Request in Warrington for 5 desktops, 4 laptops and 1 monitor			
Applicable Charges would be:			
Trip Charge	$ 50.00	1	$ 50.00
Mileage: 23 miles Billed. Saves 163 miles	$ 0.53	23	$ 12.19
Asset Disposal	$ 10.00	10	$ 100.00
Labor/Packing	$ 30.00	1	$ 30.00
Total			**$ 192.19**
#3 Department of Motor Vehicles			
Additional Ticket Request in Manassas for Secure Transport of 1 Server To DMV Headquarters in Richmond			
Applicable Charges would be:			
Trip Charge	$ 50.00	1	$ 50.00
Mileage: 115 miles Billed. Saves 84 miles	$ 0.53	115	$ 60.95
Labor/Packing	$ 30.00	1	$ 30.00
Total			**$ 140.95**

Figure 4 Sample Asset Disposal Scenarios

4.4.2 Offline Security Patching

For Devices that are not purchased through this contract or otherwise available as a part of the Services provided under this agreement, Offline Security Patching will be initiated by a Solution Request and handled as a Project. For all Offline Security Patching Projects, Iron Bow will include at a minimum:

a. Assigned Project Manager
b. Technical review or requirements completed jointly with Customer
c. Planning and scheduling completed jointly with Customer
d. Reporting and Patching status notices

Pricing for Offline Security Patching Projects will be developed based on the technical review, to determine level of effort, using the rate card (Exhibit 4.1). A price proposal will be delivered to the Customer, as coordinated with the MSI, that includes each rate proposed, their role, number of proposed hours, and schedule. Once approved by the Customer, the Software Services Manager will assign resources to execute the Offline Security Patching Project. Once completed, the ticket will be updated in Cherwell (integrated with the SMS).

Iron Bow's process is as follows for Offline Security Patching:

Baseline: Audit all off-line machines and Patch to agreed Patching level baseline; conversely, reimage all offline machines to a common image with known Patching level. This will be a manual process that will take effort to accomplish but will set us up for success moving forward. Once a solid baseline is established, Iron Bow will implement the Offline Patch Deployment Process.

- Windows Machines
  - Define Patching schedule/frequency to match VITA requirements
  - Leverage WSUS Offline Update (or other tool) to compile and download all appropriate Patches based on defined baseline OS and Office versions.
    - With Windows 10, leverage Monthly Quality Updates to manually update machines to the required Patch level and 2x per year to deploy feature updates manually.
  - Create update media (USB or DVD ISO) containing Update Installer Software and required Patches.
    - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
  - Analyze log files to ensure completion and no errors are present
  - Create Offline Machine Patching Report Data
- Mac/Android/Linux Machines
  - Define Patching schedule/frequency to match VITA requirements
    - [redacted]
    - [redacted]
    - [redacted]
  - Analyze log files to ensure completion and no errors are present.
  - Create Offline Machine Patching Report Data

4.4.3 Conference Room Support

Iron Bow will Service conference room equipment as an Enhanced Service. Support includes: break fix, coordination with 3rd Party vendors to fix equipment or connectivity issues. Description of support within this category and charges for Services, are as follows:

i. Best effort by Field Service Technicians to support End Users in getting their Device to work with conference room equipment, SLAs do not apply
ii. Smart Hands (Smart Hands charges apply if requested by a STS)
iii. If requested from Customer or Agency, Iron Bow will provide support to manage the conference room equipment and charges for such will be applied through use of the rate card (Exhibit 4.1)

4.4.4 Bring Your Own Device (BYOD) Support

Iron Bow will provide support for BYOD as an RU. All Devices must be government-owned and not personally-owned Devices. Legacy devices are excluded from the BYOD RU.

To ensure these Devices are compliant with the requirements within EUC, Iron Bow's Software and Hardware Services Team will perform the following tasks:

a. Review the Device for compliant architecture
b. Review drivers
c. Test drivers
d. Update/customize image
e. Pilot test to ensure the Device will be stable in the Environment

The BYOD service will be offered as a one-time RU charge for the above review. All BYOD Users whose Devices are deemed compliant, will be required to also purchase a Service plan to ensure the Devices are maintained.