ATTACHMENT 2 SCRM (SUPPLY CHAIN RISK MANAGEMENT) PLAN [L.29.1.3, M.2.2(2), G.6.3, H.37]

A2.1 OVERVIEW [L.30.2.2 (PARA 1-3), G.6.3 (PARA 1-3)]

MetTel's SCRM is carefully thought out with adherence to relevant standards

- SCRM Plan follows the guidance from NIST SP 800-161
- Follows the NIST SP 800-161 guidelines
- MetTel utilizes NIST's Ten (10) Supply Chain Risk Management Practices
- [redacted]

Supply Chain Risk Management (SCRM) is a discipline that addresses the threats and vulnerabilities of commercially acquired information and communications technologies within existing and planned supply chains and is used both by government and industry to better understand and reduce the risk from Information and Communications Technology (ICT) supply chains. Through SCRM, government and industry can move toward minimizing the risk to ICT and their components obtained from sources that are not trusted or identifiable as well as those that provide inferior material or parts.

MetTel's SCRM plan covers the following 5 supply chain phases:

- Design and Engineering
- Manufacturing and Assembly
- Distribution and Warehousing
- Operations and Support
- Disposal and Return

Design and Engineering: MetTel's SCRM plan uses the guidance in NIST SP 800-161 to reduce ICT supply chain risk by communicating our ICT SCRM requirements to three different types of organizations that provide ICT products and services to our Federal BSS: system integrators, suppliers, and external service providers. MetTel, based on our "Systems and Services Acquisition Policy" structures our design and engineering process to ensure that all Federal systems designs are based on using only direct suppliers who provide only Genuine Information Technology Tools (ITT). Our engineering development staff purchases products and services only from systems integrators, resellers and OEMs. MetTel requires that all Federal BSS suppliers follow our "SCRM Plan" and our "Systems and Services Acquisition Policy" before any delivery or installation and they must all have valid licenses for OEM equipment and software.

Manufacturing and Assembly: All MetTel manufacturing and assembly activities are focused on the reduction of supply chain risk. MetTel's "SCRM Plan" and the associated Systems Acquisition (SA) controls for Tiers 1 to 3, mandates that only NIST SP 800-161 ICT compliant parts, components and services be used for MetTel Federal efforts in order to reduce supply chain risk for Federal manufacturing and assembly tasks. MetTel requires that all Federal BSS suppliers follow our "SCRM Plan" and our "Systems and Services Acquisition Policy" including the appropriate Provenance SA controls before any delivery or installation. MetTel SCRM policy mandates that all ICT materials must all have valid licenses for OEM equipment and software.

Distribution and Warehousing: MetTel's "SCRM Plan" mandates that only NIST SP 800-161 compliant parts, components and services be used for Federal customer distribution and warehousing functions to reduce ICT supply chain risk. MetTel does not warehouse and/or distribute non-SCRM compliant equipment to Federal customers. NIST SP 800-161 in SCRM_PV-2 states "Tracking of provenance helps to detect unauthorized tampering and modification throughout the ICT supply chain, especially during repairs/refurbishing, for example, by comparing the updated provenance with the original baseline provenance. Tracking of provenance baselines should be performed through using configuration management mechanisms. Organizations should ensure the timely collection of provenance and change information to provide near real-time traceability as possible." MetTel's goal is to maintain as much SCRM control as feasible across the distribution and warehousing continuum as possible.

Operations and Support: MetTel's "SCRM Plan" mandates that only NIST SP 800-161 compliant parts, components and services be used for Federal customer operations and support. MetTel has a corporate commitment to reduce ICT supply chain risk by only using SCRM compliant equipment, parts and services for Federal customers. MetTel is including the appropriate SCRM clauses in all supplier contracts for Federal customers. MetTel's risk assessment process includes a focus on assessing risk to MetTel operations from the ICT supply chain perspective and determine the proper safeguards to manage and mitigate as much of that risk as possible. Operations and support are an important component of MetTel's overall risk assessment with the goal of understanding and controlling any residual ICT supply chain risk.

Disposal and Returns: To reduce supply chain risk, MetTel uses only licensed and bonded data destruction vendors for the decommissioning of defective and/or obsolete products. Our data destruction contractors have signed full and comprehensive non-disclosure agreements. The data destruction process is fully documented by serial number and a video tape is made of the entire process to ensure proper chain of custody for the ICT item being destroyed. MetTel's SCRM policy forbids the refurbishment of returned equipment for Federal customers. Returned equipment and or supplies are always exchanged under the manufacture's original warranty for new ICT equipment and/or supplies which are under contractual SCRM full lifecycle governance. MetTel makes every effort to prevent the transmission of sensitive data to unauthorized and/or unspecified parties during the disposal process as per "System Security Plan" (SSP) control SA-19 (3).

MetTel and SCRM

MetTel bases our corporate EIS SCRM strategy on the guidance contained in NIST SP 800-161 "Supply Chain Risk Management Practices for Federal Information Systems and Organizations". **Exhibit A2-1** shows the types of risks inherent it the supply chain by threat type, the actual threat and the vulnerability. MetTel's SCRM Plan addresses all three areas.

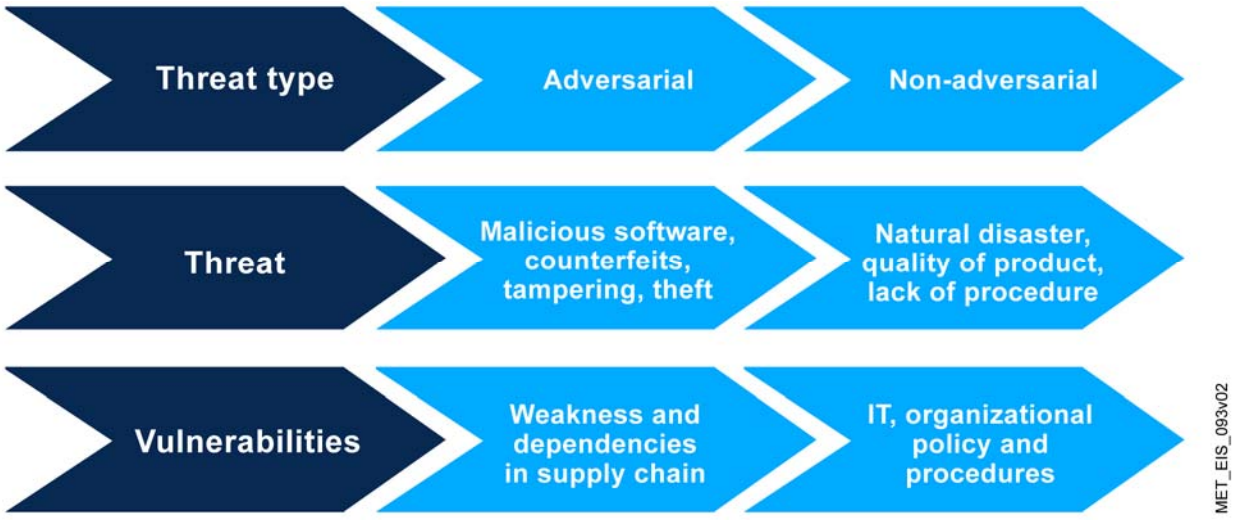


Exhibit A2-1. Supply Chain Risk Types

The expansion of the telecommunications sector, increased use of outsourcing, and development of open standards are some of the factors that present new challenges to

the security of ICT systems. These factors have resulted in emerging threats and have made protection of the ICT supply chain increasingly difficult. MetTel has a corporate commitment to SCRM, starting with Marshall Aronow, the CEO and Andoni Economou, the COO. All MetTel staff members are trained to understand these emerging threats and why SCRM is necessary to ensure the protection and viability of the MetTel Federal BSS for the EIS contract.

Supply Chain Analysis

To determine the applicability of SCRM to the MetTel BSS, our engineers are trained to comprehend on supply chain material management processes, the emerging threat, and the current ICT supply chain challenges. This background assists our staff members in assessing which BSS systems, components, software, organizational processes, and workforce issues have vulnerabilities or weaknesses that can be exploited.

MetTel's approach to an accurate SCRM assessment includes an evaluation of the origin of the product(s) and/or services, how they are distributed, and the decision-making process in the selection of the product for inclusion in our EIS BSS. The MetTel development and engineering role is to ensure that our systems engineering process is applied to all BSS components and parts of the BSS throughout their life cycle.

Life-Cycle Applicability

MetTel's management and developers are trained to apply SCRM at any point of a system's life, systematically; it is never too late or too early in a system life for a systems engineer to incorporate the SCRM process. SCRM is currently being applied to BSS materiel supply during the logistic phases, but a more effective systems engineering process will include addressing SCRM as early in the program as possible.

MetTel is following the NIST SP 800-161 guidelines which offer detailed suggestions on how and when SCRM should be integrated into the life cycle of a system. **Exhibit A2-2** shows a summary of some key steps identified in the guide that MetTel is applying to our BSS include:

Exhibit A2-2. Key Steps

#	Description
1	Determine system criticality

#	Description
2	Determine the supply chain threat
3	Select based on a "build versus buy" analysis
4	Select SCRM key practices and determine sufficiency
5	Understand the Risk Management Plan adopted by the Government Agency and the efforts they support
6	Understand the I kelihood and the consequence of insufficient SCRM practices

Exhibit A2-3. SCRM Risk Assessment

Outlined within this plan are the risk assessment activities, organizational support model, reporting and mitigation strategies that we use as a continuously improving framework and thought process for SCRM. These activities are reviewed in every aspect of the risk management cycle. By using this comprehensive process, we ensure the security and integrity of MetTel's Global Network Services as the technology and the systems evolve, or MetTel's team and procedures change.

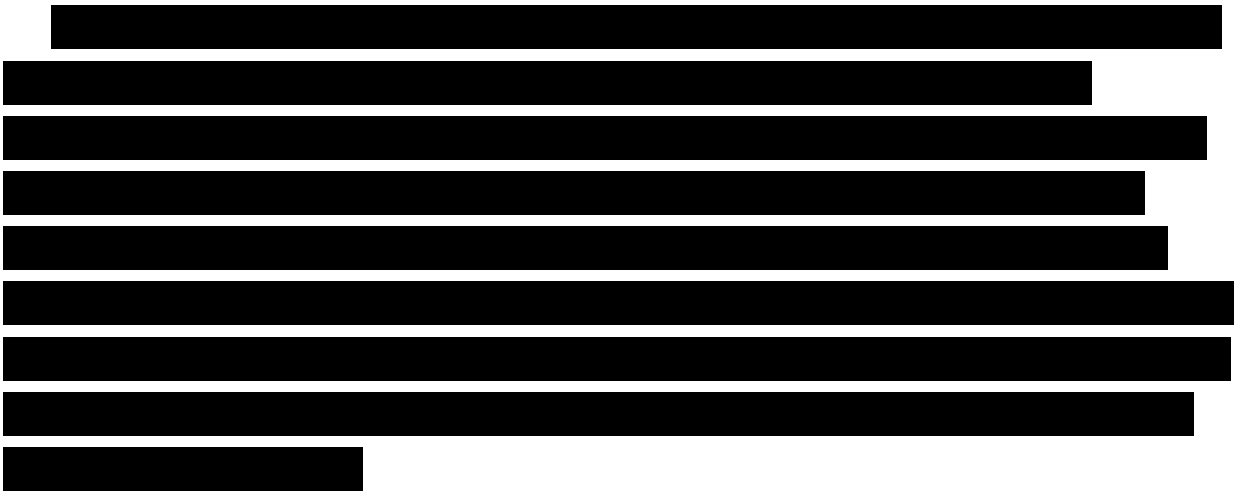
A2.2 ASSURANCE OF GENUINE INFORMATION TECHNOLOGY TOOLS [L.30.2.2(1), G.6.3(1)]

MetTel's Systems and Services Acquisition Policy strictly specifies that we solely use vendor certified resellers and/or direct suppliers who only use Genuine Information Technology Tools (ITT). This includes systems integrators, resellers and OEMs. MetTel requires that all suppliers follow our SCRM Plan before any delivery or installation and they must all have valid licenses for OEM equipment and software. Additionally SCRM language is being added to all MetTel supplier contracts in compliance with NIST SP 800-161.

MetTel only works with OEMs who exercise strict quality control and supply only vendor certified products to ensure that counterfeit or illegally modified hardware or software components are not incorporated into the OEM product(s). This strict SCRM oversight includes traceability and evidence of genuineness of ITT back to the licensed product and component OEMs, with vendor approved certificates of authenticity to be provided as part of the purchase contract.

A2.3 METTEL'S USE OF SYSTEM SECURITY ENGINEERING PROCESSES [L.30.2.2(2), G.6.3(2)]

MetTel uses strict system security engineering processes in specifying and designing a system that is protected against external threats and against hardware and software vulnerabilities.

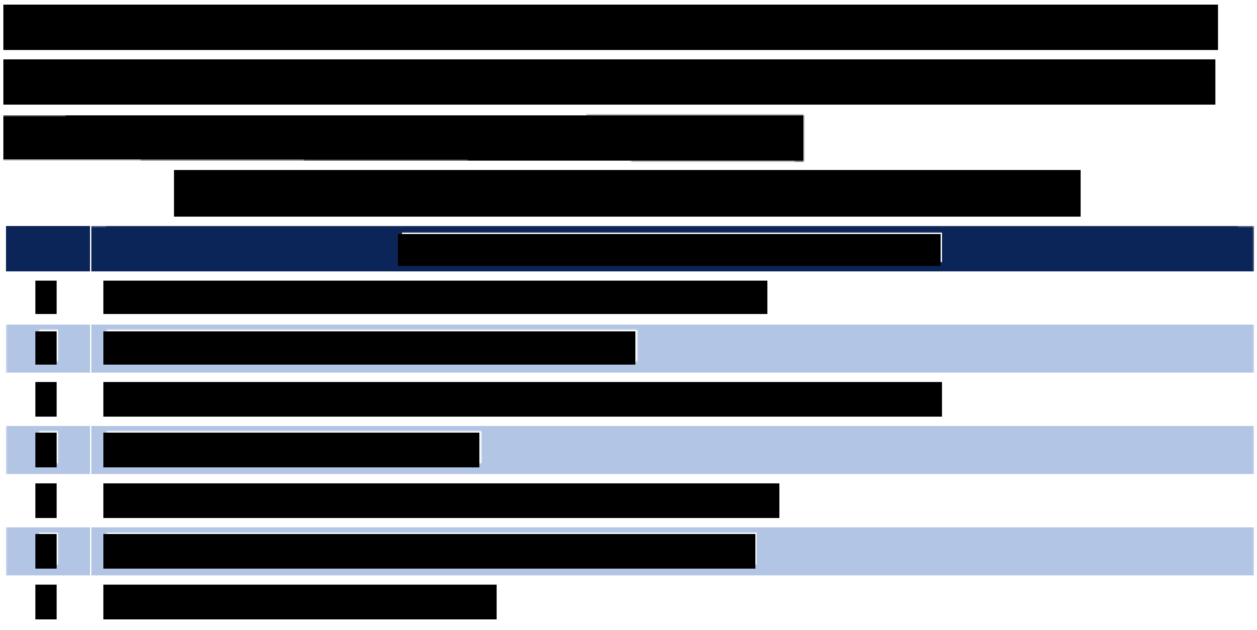


The essence of risk management is strict control and while risk management establishes the core for an effective SCRM process, MetTel's development and engineering staff understands the relationship of other systems engineering disciplines and processes to SCRM. Standard program documentation addressing software engineering practices and procedures for the MetTel EIS Portal will include the applicability of the overall SCRM process with an emphasis on standards compliance to NIST SP 800-161.

Another process that supports the protection of MetTel's supply chain is rigorous configuration management. Through MetTel's configuration control and management policies, our developers and engineers can ensure that the system's baseline is tightly controlled and any changes to it are in accordance with appropriate systems engineering processes.

A2.4 STRATEGY FOR IMPLEMENTING SCRM SECURITY REQUIREMENTS [L.30.2.2(3), G.6.3(3)]

MetTel has implemented a comprehensive supply chain risk management methodology to meet the government's EIS requirements. Our methodology addresses both physical and logical threats to the MetTel global network and the customers that MetTel serves. MetTel's SCRM policies and procedures are based on both commercial and government supply chain risk management best practices using NIST SP 800-161.



[redacted]

The security control set baseline for Moderate Impact systems provided in NIST SP 800-53 (Rev 4) including but not limited to SA-12, is our foundation and starting point for determining the needed set of security controls at the Moderate Impact Level. In many cases, customized security controls, control enhancements, and/or compensating controls will be needed to address the specific threats to and vulnerabilities of our EIS BSS. When our risk assessment determines that certain BSS components are subject to potential threats, an integrated SCRM procurement process is used to analyze potential supply chain risks and implement additional security controls and SCRM practices as needed. Efforts to control and mitigate risks are implemented throughout the information/system procurement lifecycle.

In addition to the components and processes that MetTel is directly responsible for, and as feasible; MetTel will identify 'specified supporting infrastructure beyond our system boundary' by evaluating our extended supply chain and where appropriate we will include that infrastructure in our SCRM Plan to further reduce supply chain risk. NIST SP 800-161 quotes "Dependencies on supporting or associated components that might be more accessible or easier for malicious actors to subvert than components that directly perform critical functions." MetTel interprets this to mean that risk to our ICT supply chain can come from outside our system boundary and therefore we make every possible effort to identify such risks and mitigate them to the greatest extent feasible.

[redacted]

A2.5 METTEL'S CRITICALITY ANALYSIS PROCESS [L.30.2.2(4), G.6.3(4)]

MetTel's Critical Analysis (CA) team, which is composed of members from our Change Control Board, contracts staff, developers and engineers provides oversight of our key suppliers for hardware and software components. The team's analysis includes proof of company ownership for key suppliers, manufacturer certifications to include their component manufacturers and whether the company location is on-shore or off-shore.

MetTel strictly uses only direct suppliers who provide only trusted Information Technology Tools (ITT). This includes systems integrators, resellers and OEMs. MetTel requires that all suppliers follow the SCRM Plan before any delivery or installation and they must all have valid licenses for OEM equipment and software.

MetTel has strict policies that all equipment has been purchased from reputable vendors who provide certificates of authenticity and warranties for all the equipment and components they provide. These certificates and warranties are passed along to the customer as part of the MetTel sales agreement.

Additionally, MetTel only works with OEMs that exercise strict quality control to ensure that counterfeit or illegally modified hardware or software components are not incorporated into the OEM product and include traceability and evidence of genuineness of ITT back to the licensed product and component OEMs.

MetTel corporate policy ensures that SCRM clauses are inserted into all purchasing agreements with vendors and that the vendors supply us with the appropriate SCRM documentation as specified in NIST SP 800-161. MetTel maintains full documentation and audit trails with all of our vendors to ensure full accountability throughout the purchasing and acquisition lifecycle.

MetTel does not purchase anything or enter into contractual relationships with unknown and/or unidentified sources under any circumstances. Our corporate reputation depends on our integrity and the integrity of our supply chains.

A2.6 HOW METTEL ENSURES PRODUCTS AND COMPONENTS ARE NOT REPAIRED AND SHIPPED AS NEW [L.30.2.2(5), G.6.3(5)]

MetTel has strict policies that all equipment has been purchased from reputable vendors who provide certificates of authenticity and warranties for all the equipment and components they provide. These certificates and warranties are passed along to the customer as part of the MetTel sales agreement.

To counter the risk of inadvertently get repaired components instead of new, MetTel takes following steps:

[redacted]

A2.7 HOW METTEL ENSURES SUPPLY CHANNELS ARE MONITORED FOR COUNTERFEIT [L.30.2.2(6), G.6.3(6)]

MetTel fully understands that ICT supply channels are filled with counterfeit merchandise, components and spare parts. A circuit board purchased from a public Internet auction site will cost a fraction of the price of the genuine item(s) purchased from the OEM and/or approved resellers.

MetTel strictly follows our System and Services Acquisition Policy and our SCRM Policy which mandates purchasing solely from publically known sources who provide

genuine “brand name” equipment with new, genuine components and complete with warranties, certifications, and support.

MetTel strictly does not repair equipment and resell and/or replace. If non-functional equipment cannot be repaired by the OEM or vendor under product warranties and contractual obligations, it is destroyed by a certified data destruction provider with photographic evidence provided.

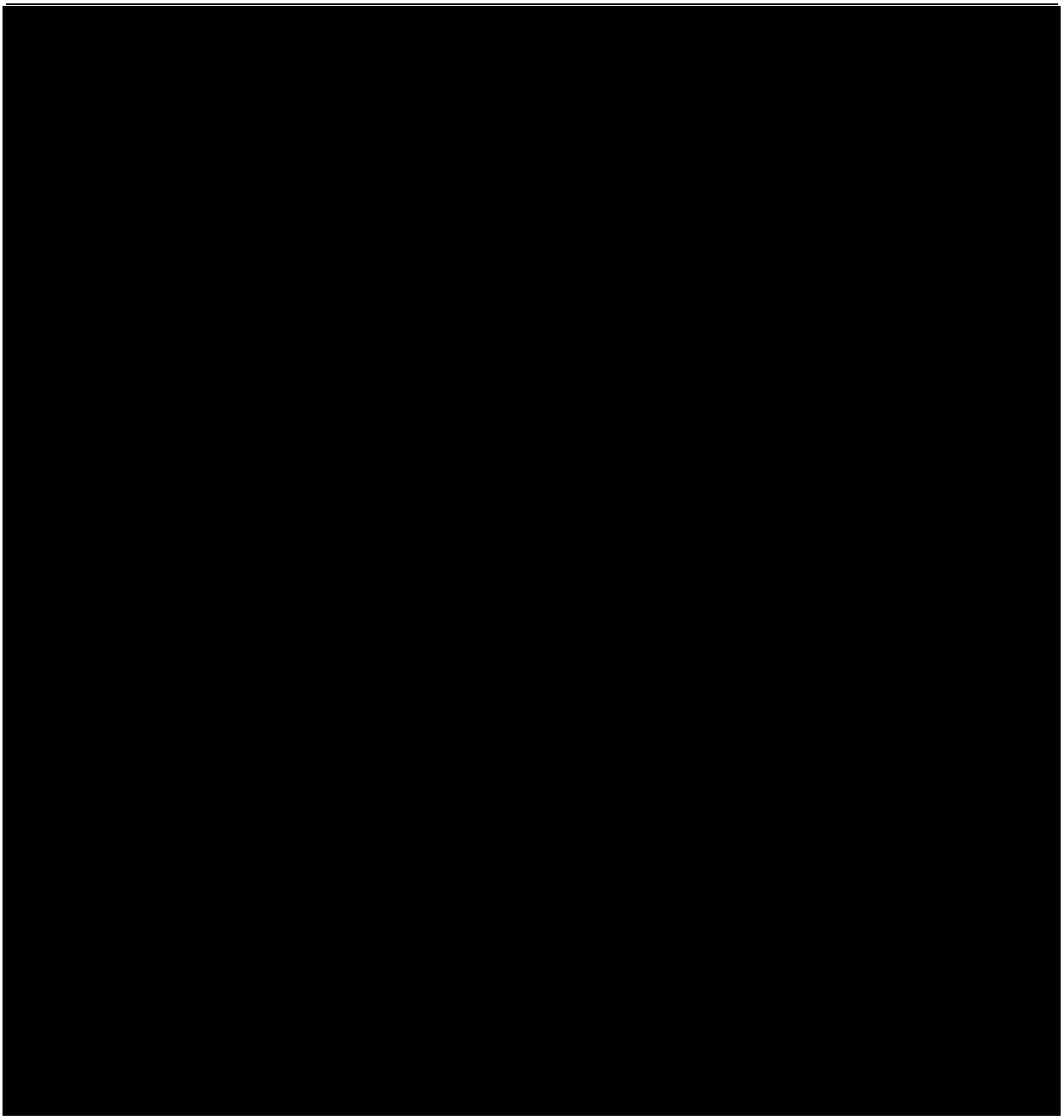


Exhibit A2-5. ICT SCRM Activities

A2.8 METTEL'S PHYSICAL AND LOGICAL DELIVERY MECHANISMS [L.30.2.2(7), G.6.3(7)]

MetTel fully understands that the delivery/shipment of any hardware/software provides opportunities for hackers to compromise systems along the supply chain and system or element product life-cycle. MetTel strengthens our delivery mechanisms to

ensure that opportunities for unauthorized access or exposure to the element, processes, and systems are prevented. To further protect confidential information regarding business operations within MetTel, procedures for both internal and external personnel are strictly defined and reviewed on a routine basis.

[redacted]

Additionally, MetTel requires valid and current certificate(s) of insurance for all deliveries to both our headquarters and data center locations.

A2.9 METTEL'S OPERATIONAL AND DISPOSAL PROCESSES [L.30.2.2(8), G.6.3(8)]

MetTel follows our Systems and Services Acquisition Policy and SCRM Policy by selecting publically known vendors of software, hardware or services and managing the maintenance, upgrade, patching, element replacement, or other sustainment activities through them only to limit opportunities for knowledge exposure, data release, or system compromise.

[redacted]

A2.10 METTEL RELATIONSHIP TO MANUFACTURER [L.30.2.2(9), G.6.3(9)]

MetTel in accordance with our System and Services Acquisition Policy and our SCRM Policy only purchases ICT equipment and/or products from OEMs, OEM authorized resellers and OEM authorized partners/distributors.

MetTel corporate policy ensures that SCRM clauses are inserted into all purchasing agreements with vendors and that the vendors supply us with the appropriate SCRM documentation as specified in NIST SP 800-161. MetTel maintains full documentation and audit trails with all of our vendors to ensure full accountability throughout the purchasing and acquisition lifecycle.

MetTel does not purchase anything or enter into contractual relationships with unknown and/or unidentified sources under any circumstances. Our corporate reputation depends on our integrity and the integrity of our supply chains.

A2.11 METTEL'S SOFTWARE WARRANTY [L.30.2.2(10), G.6.3(10)]

MetTel's SCRM Plan includes MetTel's expressed warranty and appropriate vendor warranties that the software will be free from all computer viruses, worms, time-outs, time bombs, back doors, disabling devices and other harmful or malicious code intended to or which may damage, disrupt, inconvenience or permit access to the software user's or another's software, hardware, networks, data or information. [redacted]

MetTel strictly follows our System and Services Acquisition Policy and our SCRM Policy which mandates purchasing solely from publically known sources who provide genuine "brand name" software complete with warranties, certifications, and support, which are then passed to the customer/end-user.

MetTel requires that all software products purchased, come complete with vendor certification and warranties. We maintain an automated system which tracks software licensing to ensure that MetTel is in full compliance with all software licensing requirements. MetTel will only propose Commercial-Off-the-Shelf (COTS) components with standard commercial warranties that are consistent with clause 52.246.17. In the case of standard commercial warranties that exceed one year, the government will receive the additional term(s) of the commercial warranty.

A2.12 HOW METTEL ENSURES INDEPENDENT VERIFICATION AND VALIDATION OF ASSURANCES [L.30.2.2(11), G.6.3(11)]

[redacted]

A2.13 METTEL'S SUBCONTRACTORS [L.30.2.2 & G.6.3 SECOND TO LAST PARAGRAPH]

MetTel's contractual policy, as approved by our leadership and General Counsel mandates the insertion of a SCRM paragraph in all subcontracts agreements before the final portion of the contract language.

MetTel fully understands that the insertion of SCRM contract language is required for all circumstances where a subcontractor to MetTel provides a critical component or part of the MetTel's supporting BSS infrastructure.

All MetTel subcontractors providing critical components or services to/for our BSS are identified and required to provide all necessary information to complete the SCRM Plan in association with the contractor. MetTel inserts SCRM language into all of our contracts and requires the full compliance of the subcontractor. MetTel further acknowledges that suppliers of COTS components (hardware and/or software) are considered subcontractors for the EIS contract.

A2.14 UPDATES TO SCRM PLAN [L.30.2.2 LAST PARAGRAPH, G.6.3 LAST PARAGRAPH]

MetTel acknowledges that we fully comply with NIST SP 800-161 "Supply Chain Risk Management Practices for Federal Information Systems and Organizations". MetTel will update our SCRM Plan to include any future changes to the NIST SCRM Guidelines and all such modifications shall be implemented at no cost to the government. All updated plans will be provided to the government upon completion.