ATTACHMENT 1 RISK MANAGEMENT FRAMEWORK PLAN [L.29.2.2, M.2.1(4)]

According to a 2015 study conducted by the Ponemon Institute, the annual cost of cybercrime to an individual company has more than doubled since 2010 to more than $13 million, and the average number of successful cyber-attacks has tripled to an average of 160 per week. With these staggering numbers, it is clear the effectiveness of security operations needs improvement in limiting the impact and in decreasing the time to resolve such events across Government and industry. As a microcosm of these national challenges, DHS, their partners, and their customers are proactively adapting cybersecurity measures to meet this new and ever-evolving environment. MetTel, by providing services under the EIS contract, is subject to all the applicable federal and agency-specific IT security directives, standards, policies, and reporting requirements. MetTel will comply with Federal Information Security Management Act (FISMA) associated guidance and directives to include Federal Information Processing Standards (FIPS), NIST SP 800 series guidelines, GSA IT security directives, policies and guides, and other appropriate government-wide laws and regulations for protection and security of government IT**. Appendix A** provides the listing of compliance references. This list is dynamic and will be updated as required.

Through the contract period of performance, MetTel will timely and consistently implement new threat countermeasures to address these security concerns. Because eliminating all threats is impossible, determining the possible exposure and how best to manage risk is an essential task. MetTel's structured approach to Risk Management:

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

Appendix B presents the deliverables produced during the execution of the risk management approach to achieve the assessment and authorization process.

The steps required by the risk management framework (shown in **Exhibit A1-1**) enable MetTel to make the most informed risk decision.

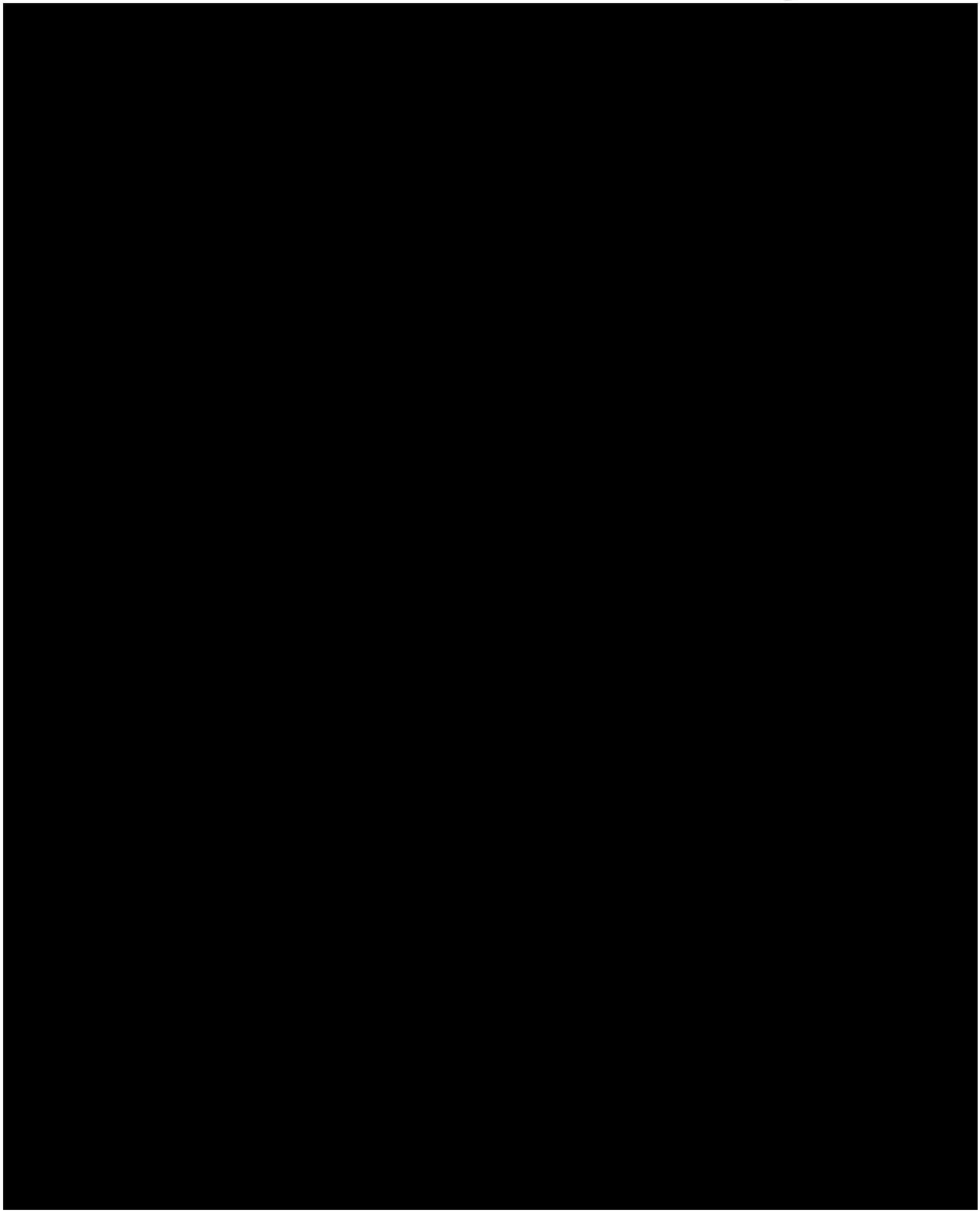
Exhibit A1-1. Risk Management Framework

Task 1: Determine the Security Categorization. The security categorization of the system was gleaned from information in Section C.1.8.7.2 of the RFP as moderate. The Security categorization is defined as:

EIS = {(Confidentiality, “moderate”), (Integrity, “moderate”),
(Availability, “moderate”)}

This categorization enabled MetTelto identify the minimum controls to be applied in accordance with NIST 800-53 rev 4 (**Exhibit A1-3**).

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.



Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

Exhibit A1-3. Minimum Required Moderate-Level Controls as Defined in NIST 800-53 rev 4

ID	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted] The RFP defines the accreditation boundary as where MetTel's services connect to the Participating Agency's (PA's) user terminals/equipment. [redacted] At a minimum, the system has a new security A&A conducted and approved by GSA every 3 years or when a significant change impacts the security posture of the system, as defined in NIST SP 800-37.

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

Exhibit A1-4. Assessment and Authorization Boundary and Traffic Flow

[redacted] The registration of the system is completed by the development of the System Security Plan (SSP) in accordance with NIST 800-1 rev 1. The SSP identifies all the security requirements of the system and describes the controls in place or planned as well as the responsibilities and expected behavior of all individuals accessing the system. At a minimum, the SSP includes all appendices and attachments identified within the Task Order.

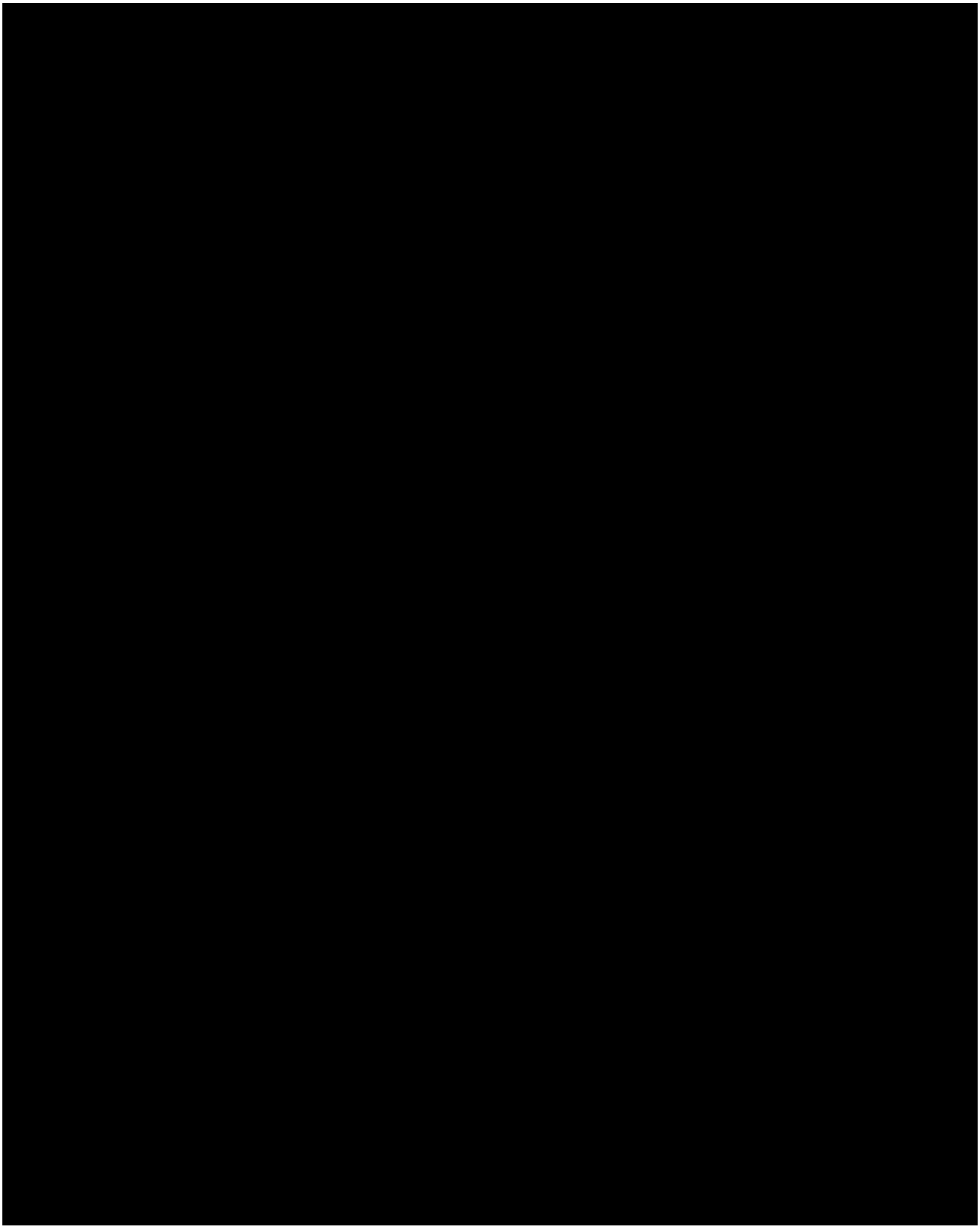
Our access control policies and implementation ensure that only personnel who have undergone and successfully completed security and/or contractor fitness checks may have logical and/or physical access to Government information or the MetTel

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

Federal BSS that falls within the approved A&A boundary. [redacted]

[redacted] identifies the security controls to be placed in the system. The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, Executive Orders, policies, standards, or regulations. Once the common controls from NIST SP 800-53 rev.4.are identified and approved, they are divided into sub-categories to identify Baseline Controls from NIST SP 800-53 rev 4. Due to the nature of services and the protection of National Security Systems and information, MetTel includes classification overlays with additional controls required by CNSSI 1253.

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.



Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

Managing geographically dispersed systems can present challenges that can be compounded when rapid changes are not fully documented or do not receive a thorough review. The MetTel team has developed change management as an organizational competency, a competitive advantage in a quickly evolving business world. Change management increases the success of organizational change and project initiatives by developing and applying a structured framework of methods, tools, and processes and managing change from a current state to a future state.

Change management helps the PA increase the probability of maintaining control and understanding of their dynamic environment with any scale of change. MetTel's flexible methodology enables:

- Integration of individual, organizational, and enterprise-wide change management for a holistic approach
- Identifying Configuration Items (CIs) – (Configuration Identification)
- Controlling changes to CIs – (Configuration Control)
- A structured approach with easy-to-use tools and resources
- Determining that a system complies with its specifications – (Configuration Audit)
- Documenting the development status of all configuration items at any point in time – (Configuration Status Accounting)
- World-class training for all levels of the organization

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

- Industry-leading best practices
- Easy-to-use, turnkey tools and resources for practitioners, managers, and executives

[redacted]

MetTel uses best practices when implementing security controls within the information system to include system and software engineering methodologies, security engineering principles, and secure coding techniques. In addition, MetTel will ensure that mandatory

[redacted]

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

configuration settings are established and implemented on information technology products in accordance with Federal and organizational policies. Controls are documented in the SSP after they have been implemented. A body of evidence is captured to identify how the control has been implemented for the system or subsystems.

The SSP template includes a section titled Security Controls Detail and Comment to document the implementation of security control requirements for each of the 17 security control families as well as who is responsible for implementing the control.

Note – The details and comments contained within the completed SSP, as well as the applicable Security Requirements SSP Workbook (provided as an attachment to the SSP), are considered the information of record for the description of implemented security controls for the system. **Exhibit A1-9** provides an example SSP template.

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

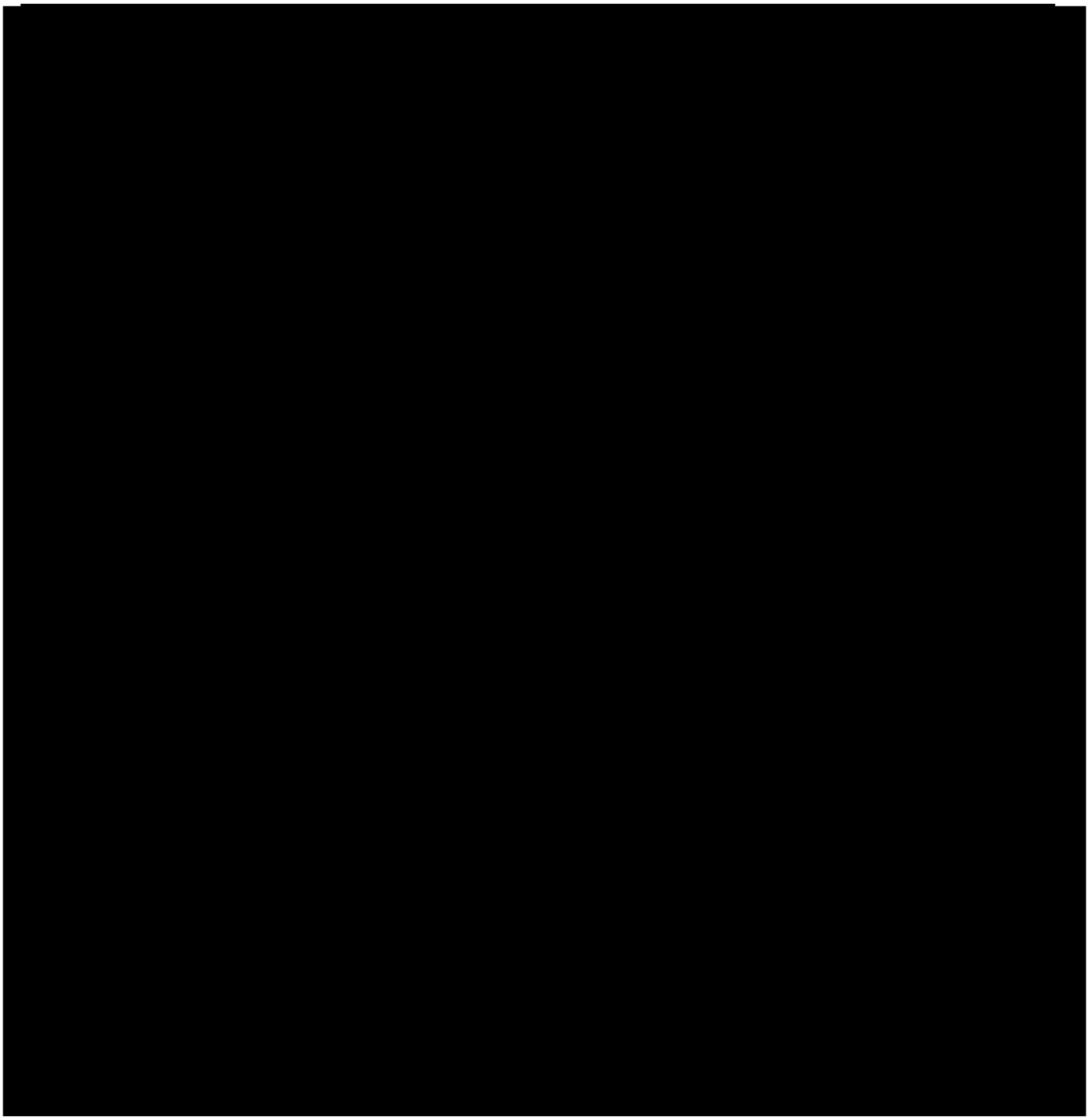


Exhibit A1-9. SSP Template Example

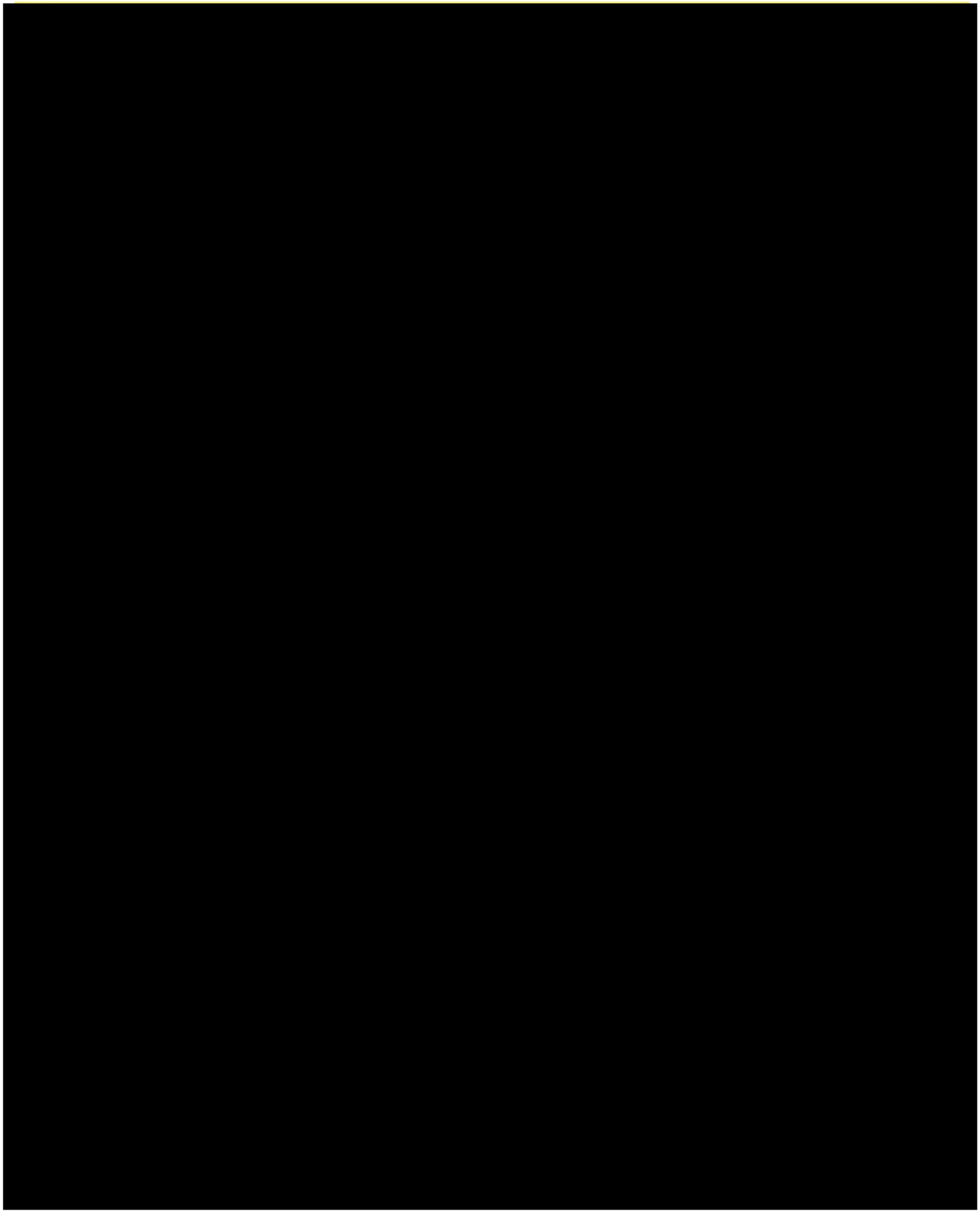
[redacted]

[redacted]. Once controls have been implemented and documented in the SSP, they must be assessed for effectiveness. [redacted]

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted] Besides being mandated by Federal policies, assessments are beneficial for improving situational awareness, providing insight and data, and identifying control system threats and vulnerabilities. Upon request, we will provide any documentation, physical access, and logical access required to support the completion of the A&A.

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.



Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

[redacted]

Exhibit A1-11. Example Risk Assessment Checklist

Control assessment and analysis identifies controls deemed as satisfying or not satisfying the control objectives. This is indicated in the Security Assessment Report (SAR) as:

- Satisfied (S)
- Other Than Satisfied (O)

A finding of ***Satisfied*** indicates that, for the portion of the security control addressed by the determination statement, the assessment information obtained (i.e., evidence collected) meets the objective producing a fully acceptable result. A finding of ***Other***

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

Than Satisfied indicates that, for the portion of the security control, potential anomalies in the operation or implementation of the control may need to be addressed by the System Owner.

[redacted]

The SAR is one of three key documents in the security authorization package (see **Exhibit A1-12**) developed for authorizing officials and includes:

a) Executive Summary of the control assessment findings and associated risks

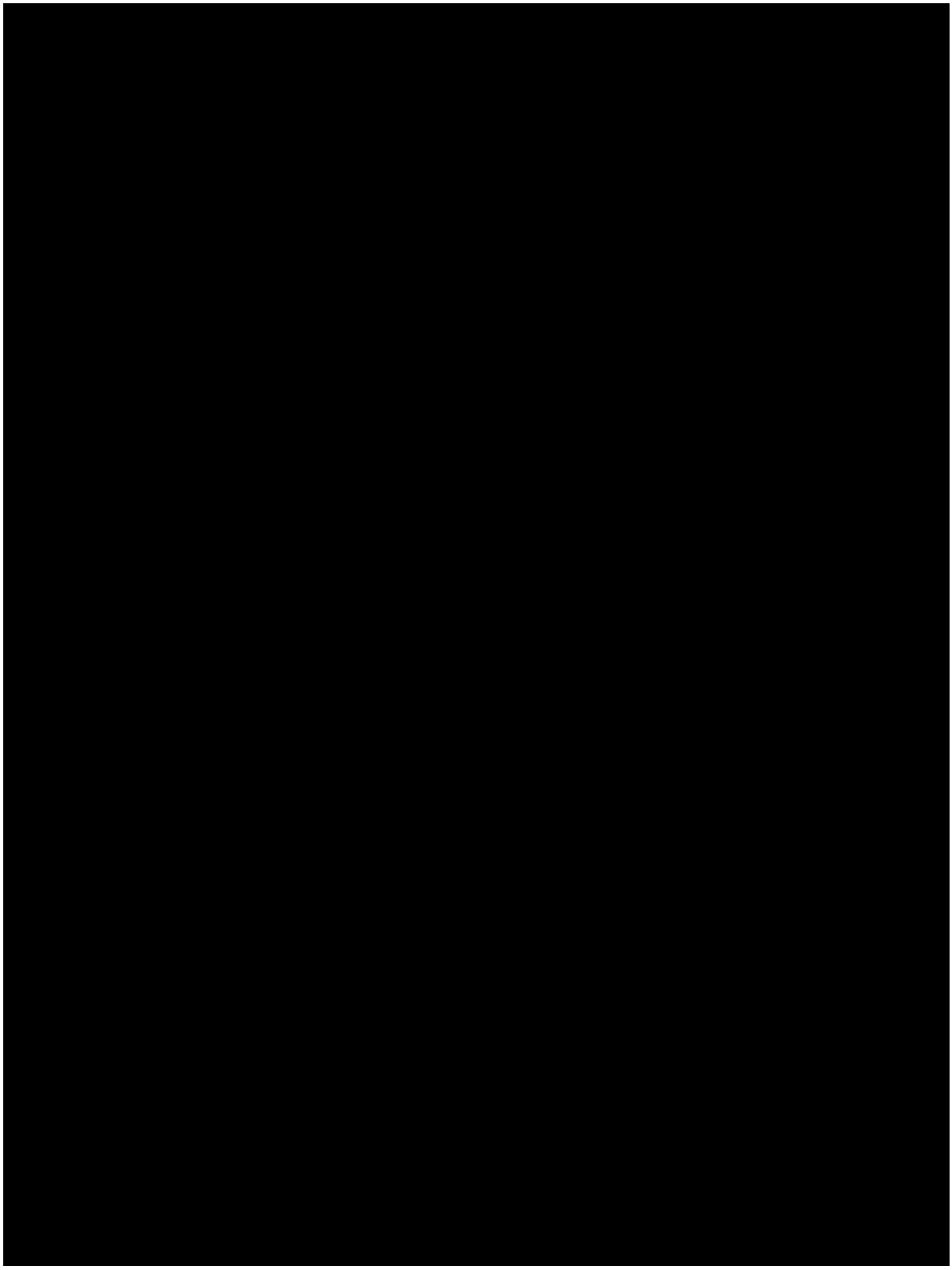
b) Executive Summary of technical testing/scanning with associated summary of vulnerabilities detected with associated severity

c) Information from the assessor necessary to determine the effectiveness of the security controls employed within or inherited by the information system based on the assessor's findings

d) Risks associated with controls found not to be effectively implemented

e) Recommendations for mitigating risks and remediating weaknesses

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.



Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

Exhibit 1A-13 shows an example SAR form.

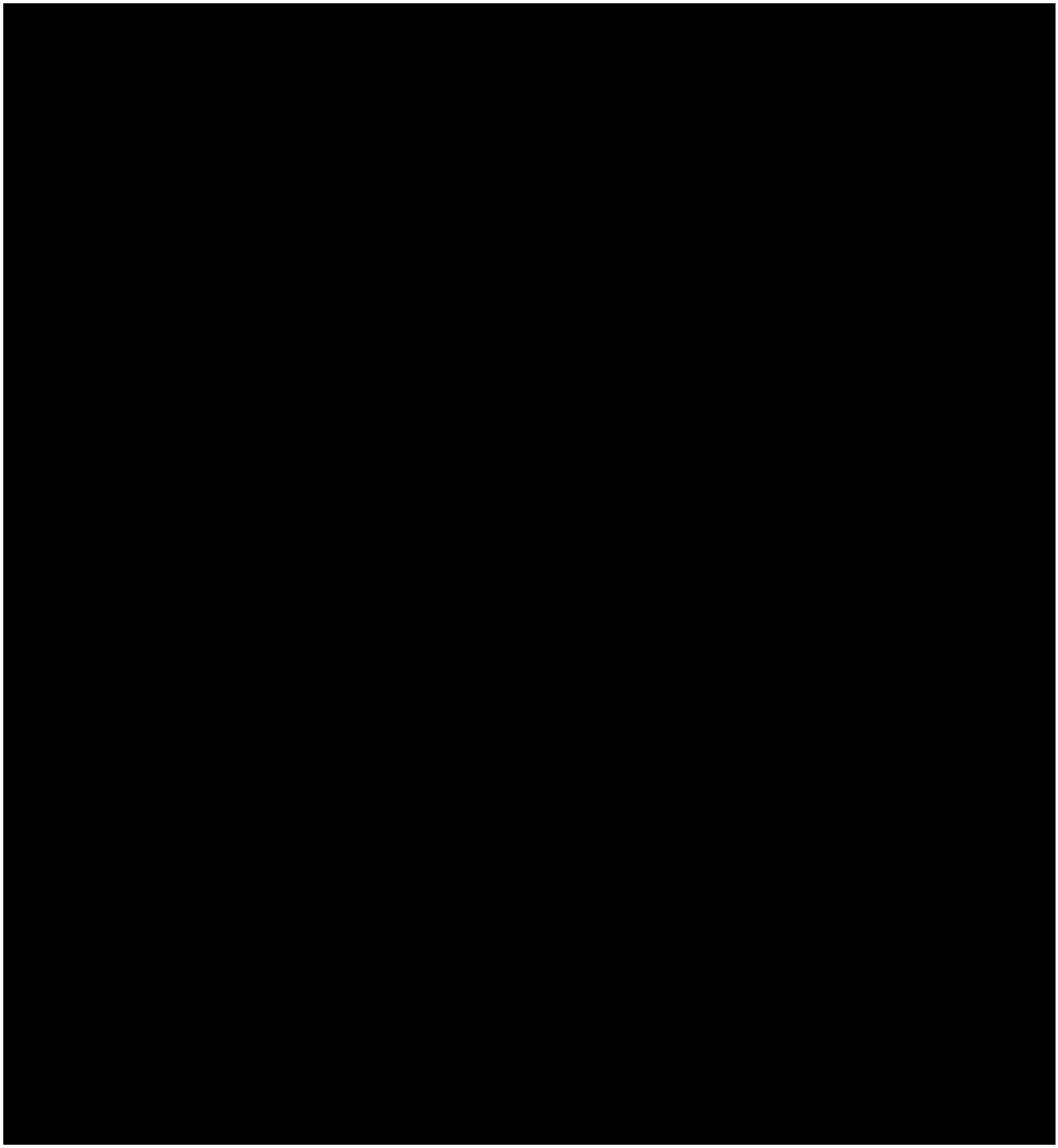


Exhibit A1-13. SAR Example

The results of the assessment and draft Plan of Action and Milestones (POA&M) are coordinated, as appropriate, with the DHS CISO, CIO, and Risk Executive. The manner in which DHS has implemented the Risk Executive Function determines the coordination process. Depending on the system, coordination may be required with

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

Agency OCIO personnel. These individuals review the risks and provide advice or recommendations to the Authorizing Official. The CISO or ISSO assembles these recommendations into an Authorization Recommendation Letter.

The System Owner assembles the security authorization package, which must contain at a minimum:

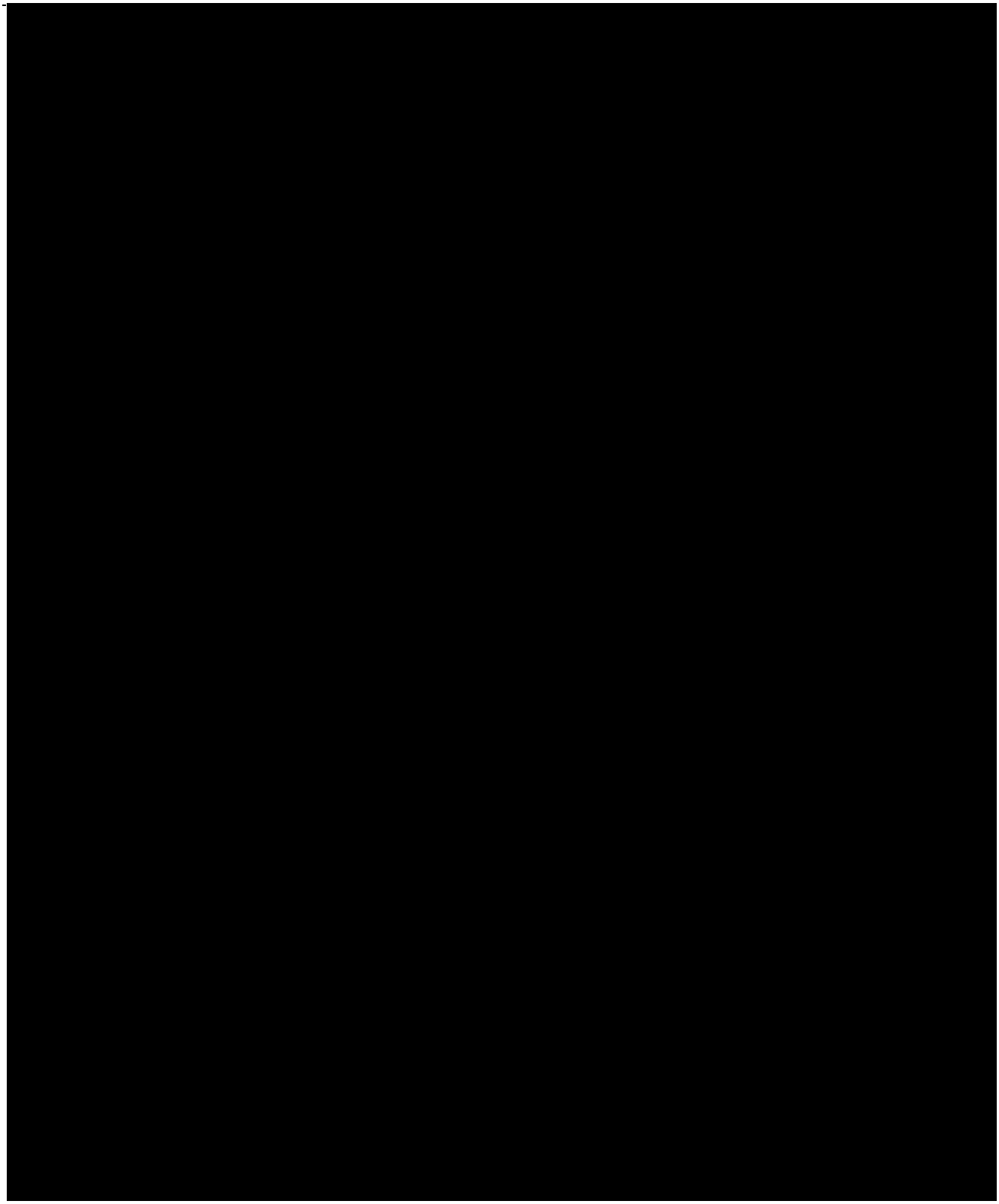
- System Security Plan (with associated appendices)
- Security Assessment Report
- Plan of Action and Milestones
- Continuous Monitoring Plan
- Authorization Recommendation

The information in these documents is used by authorizing officials to make risk-based authorization decisions.

[redacted]

With the technology sector continuously producing new hardware, software, and firmware, information systems are in a constant state of change. Thus, an effective security monitoring program must be in place. [redacted] Most routine changes to an information system or its environment of operation can be handled by the organization's continuous monitoring program, thus supporting on-going authorization and near-real-time risk management. **Exhibit A1-15** illustrates how operational security contributes to continuous monitoring.

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.



Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

All security controls employed within and inherited by the information system are assessed during the initial security authorization. Subsequent to the initial authorization, however, a subset of the most critical technical, management, and operational security controls are assessed during continuous monitoring. The selection of security controls to monitor and the frequency of monitoring is based on the monitoring strategy developed by MetTel with input from the information system owner and/or common control provider and approved by the GSA and PA. For on-going security control assessments, assessors have the required degree of independence as determined by the Authorizing Official.

Exhibit A1-15. Continuous Monitoring Process Overlap with Operational Security

The results of the continuous monitoring activities are provided to the information system owner and common control provider in an updated SAR. Based on their findings, they initiate remediation actions and the security plan, SAR, and POA&M are updated. This facilitates the near-real-time management of risks associated with the operation and use of the information system.

The security status of the information system (including the effectiveness of security controls employed within and inherited by the system) is consistently reported to the Authorizing Official and other appropriate organizational officials in accordance with the monitoring strategy. At a minimum, the system security deliverables specified by the particular Task Order are provided quarterly and on an annual basis or when significant changes, as defined in NIST SP 800-37, occur.

In addition, we support the Government, or agents acting on the behalf of the Government, in the execution of manual or automated audits, scans, reviews, or other

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

inspections of our IT environment that provide or facilitate services for the Government. We support automated scans by Government personnel or agents acting on behalf of the Government using Government equipment and Government-specified tools.

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

APPENDIX A: COMPLIANCE REFERENCES

Guidance Type	Compliance Documents
Acts and Presidential Directives	• Federal Information Security Management Act (FISMA) of 2002; (44 U.S.C. Section 301. Information Security) available at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf. • Federal Information Security Modernization Act of 2014; (to amend Chapter 35 of 44 U.S.C.) available at: https://www.congress.gov/113/bills/s2521/BILLS-113s2521es.pdf. • Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996," available at: https://www.fismacenter.com/clinger%20cohen.pdf. • Privacy Act of 1974 (5 U.S.C. § 552a). • Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and contractors," August 27, 2004; available at: http://www.idmanagement.gov/.
OMB Circulars and Memorandum	• OMB Circular A-130, "Management of Federal Information Resources," and Appendix III, "Security of Federal Automated Information Systems," as amended; available at: http://www.whitehouse.gov/omb/circulars_a130_a130trans4/. • OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies" (Available at: http://www.whitehouse.gov/omb/memoranda_2004). • OMB Memorandum M-14-03, "Enhancing the Security of Federal Information and Information Systems" (Available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf.)
FIPS PUB	• FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems" • FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems" • FIPS PUB 140-2, "Security Requirements for Cryptographic Modules"
NIST Special Publications	• NIST Special Publication 800-18 Revision 1, "Guide for Developing Security Plans for Federal Information Systems" • NIST Special Publication 800-30 Revision 1, "Guide for Conducting Risk Assessments" • NIST Special Publication 800-34 Revision 1, "Contingency Planning Guide for Federal Information Systems" • NIST SP 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach" • NIST SP 800-40 Revision 3, "Guide to Enterprise Patch Management Technologies" • NIST SP 800-41 Revision 1, "Guidelines on Firewalls and Firewall Policy" • NIST SP 800-37 Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach" • NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems" • NIST SP 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations" • NIST SP 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans"

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

Guidance Type	Compliance Documents
	• NIST SP 800-58 "Security Considerations for Voice Over IP Systems" • NIST SP 800-60 Revision 1, "Guide for Mapping Types of Information and Information Systems to Security Categories" • NIST SP 800-61 Revision 2, "Computer Security Incident Handling Guide"NIST SP 800-88 Revision 1, "Guidelines for Media Sanitization" • NIST SP 800-94 "Guide to Intrusion Detection and Prevention Systems" • NIST SP 800-128, "Guide for Security-Focused Configuration Management of Information Systems" • NIST SP 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations" • NIST SP 800-144 "Guidelines on Security and Privacy in Public Cloud Computing" • NIST SP 800-160 "Systems Security Engineering" • NIST SP 800-161, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations" • NIST SP 800-171, "Protecting Controlled Unclassified Information in the Nonfederal Information Systems and Organizations"
Committee Reports	• Committee on National Security Systems (CNSS) Policy No. 12, National Information Assurance Policy for Space Systems Used to Support National Security Missions. • Committee on National Security Systems (CNSS) Policy No. 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems. • Committee on National Security Systems Instruction 1253 (CNSSI No. 1253), Security Categorization and Control Selection for National Security Systems • Committee on National Security Systems Instruction (CNSSI) No. 5000, "Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony"
Department of Defense Instruction (DODI)	• DODI 8500.01 "Cybersecurity" • DODI 8510.01 "Risk Management Framework (RMF) for DOD Information Technology (IT)" • DOD Cloud Computing Security Requirements Guide (SRG)
Intelligence Community Directive (ICD)	• ICD 503, "Intelligence Community Information Technology Systems Security: Risk Management, Certification and Accreditation" • ICD 703, "Protection of Classified National Intelligence, Including Sensitive Compartmented Information" • ICD 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information" • ICD 705, "Sensitive Compartmented Information Facilities" • ICD 731, "Supply Chain Risk Management" • Other agency-specific policies, directives and standards as identified at the TO level.

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

APPENDIX B: NEAR-TERM DELIVERABLES AFTER AWARD

ID	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
1	NIST SP 800-53 R4; PL-2	System Security Plan (SSP)	Initial: Within 30 days of Notice to Proceed (NTP) Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
2	NIST SP 800-37 R1	Security Assessment Boundary and Scope Document (BSD)	Initial: Within 15 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
3	NIST SP 800-53 R4; CA-3	Information System Interconnection Security Agreements (ISA)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
4	NIST SP 800-53 R4; AC-1	GSA NIST 800-53 R4 Control Tailoring Workbook	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
5	NIST SP 800-53 R4; AC-1	GSA NIST SP 800-53 R4 Control Summary Table	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
6	NIST SP 800-53 R4; PL-4	Rules of Behavior (RoB)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
7	NIST SP 800-53 R4; CM-8	System Inventory	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
8	NIST SP 800-53 R4; CP-2	Contingency Plan (CP)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
9	NIST SP 800-53 R4; CP-4	Contingency Plan Test Plan (CPTP)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
10	NIST SP 800-53 R4; CP-4	Contingency Plan Test Report (CPTR)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
11	NIST SP 800-53 R4; AR-2, AR-3 and AR-4	Privacy Impact Assessment (PIA)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
12	NIST SP 800-53 R4; CM-9	Configuration Management Plan (CMP)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
13	NIST SP 800-53	Incident Response Plan	Initial: Within 30 days of NTP	GSA COR/ISSO

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.

ID	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
	R4; IR-8	(IRP)	Update: Annually from contract award and when significant changes occur	
14	NIST SP 800-53 R4; IR-3	Incident Response Test Report (IRTR)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
15	NIST SP 800-53 R4; SA-12 and NIST SP 800-161	Supply Chain Risk Management (SCRM) Plan	Initial: With the proposal Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
16	NIST SP 800-53 R4; CA-7	Continuous Monitoring Plan	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
17	NIST SP 800-53 R4; CA-5	Plan of Action and Milestones (POA&M)	Initial: With the Security A&A package Update: Quarterly Note: Critical and High vulnerabilities shall be updated monthly	GSA COR/ISSO
18	NIST SP 800-53 R4; CA-7 and RA-5	Independent internal and external penetration tests and reports	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
19	NIST SP 800-53 R4; SA-11	Code Review Report (If applicable)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
20	NIST SP 800-53 R4; CA-2	Annual FISMA Assessment	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
21	NIST SP 800-53 R4; CM-6	SCAP Common Configuration Enumerations (CCE) Report	Initial: With the Security A&A package Update: Monthly (end of month)	GSA COR/ISSO
22	NIST SP 800-53 R4; CM-8	SCAP Common Platform Enumeration (CPE) Report	Initial: With the Security A&A package Update: Monthly (end of month)	GSA COR/ISSO
23	NIST SP 800-53 R4; CM-8	SCAP Common Vulnerabilities and Exposures (CVE)	Initial: With the Security A&A package Update: Monthly (end of month)	GSA COR/ISSO

Use or disclosure of data contained on this page is subject to the restrictions on the title page of this proposal.