ATTACHMENT 2 MTIPS RISK MANAGEMENT FRAMEWORK PLAN [L.29.2.2, C.2.8.4.5]

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 over $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 to limit the impact and decrease the time to resolve such events across Government and industry. 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.

A key component of our secured infrastructure is the Managed Trusted Internet Protocol Service (MTIPS), which helps reduce the number of Internet connections in Government networks and provides standard security services to all Government users. At its core, an MTIPS is comprised of a SOC, EINSTEIN enclaves, traffic scanners, and event processing systems. Through the contract period of performance, the MetTel team is expected to implement an MTIPS 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:

[redacted]

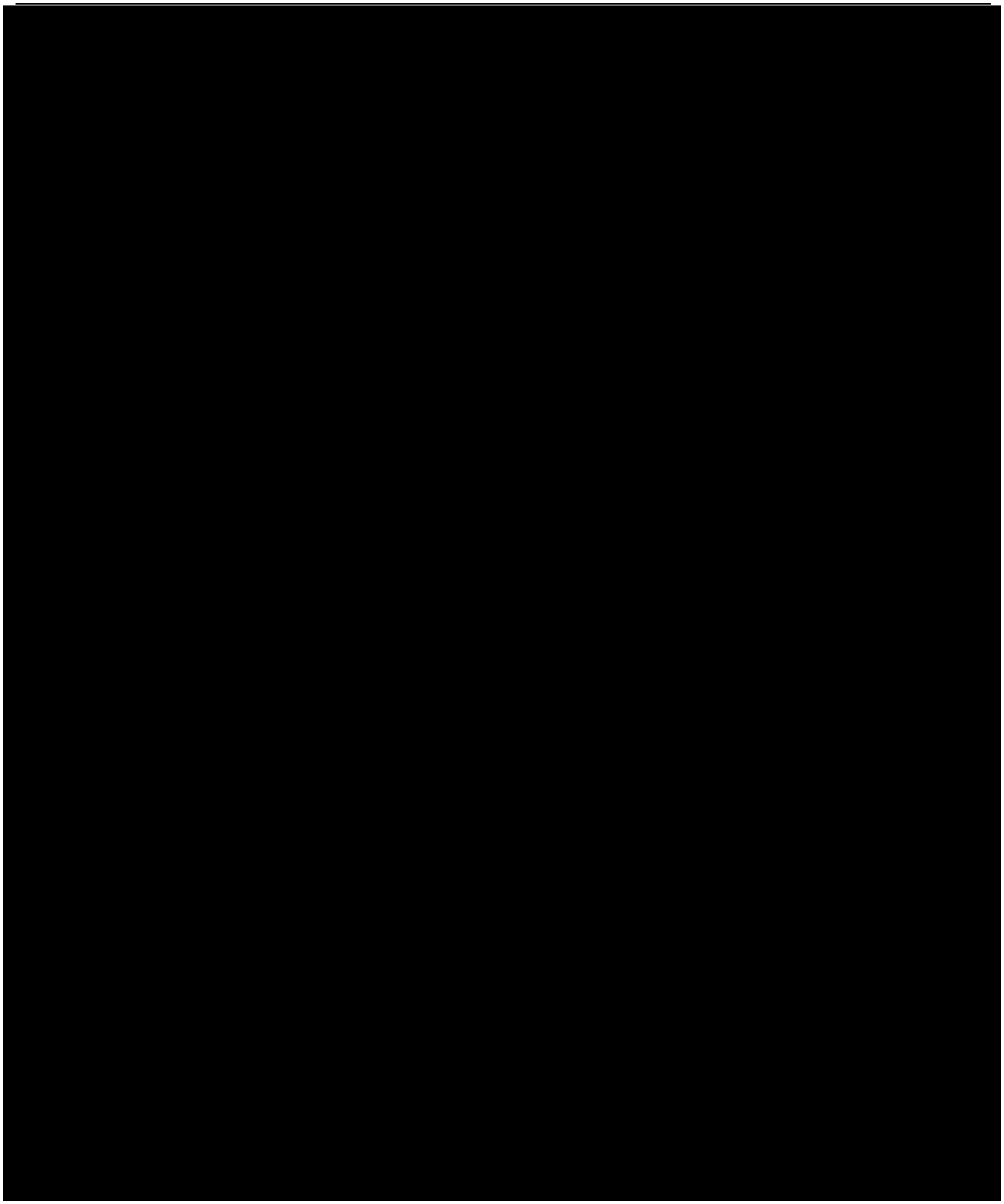
Appendix B presents the deliverables produced during the execution of the risk management approach to achieve the assessment and authorization process.

[redacted]

Exhibit A2-1. Risk Management Framework

The steps required by the risk management framework (shown in Exhibit A2-1) enable MetTel to make the most informed risk decision.

[redacted]



The MTIPS security categorization was gleaned from information in Section C.2.8.5.4 of the RFP as high-impact. The

system is categorized as:

MTIPS = {(Confidentiality, “high”), (Integrity, “high”),
(Availability, “high”)}

This categorization enabled the MetTel team to identify the minimum controls to be applied in accordance with NIST 800-53 rev 4 (**Exhibit A2-3**). We It is understood that these are the base controls and are fully prepared to discuss which specific controls the Participating Agency (PA) would like applied at the time of award.

Exhibit A2-3. Minimum Required High-Level Controls as Defined in NIST 800-53 rev4

[redacted] The RFP defines the accreditation boundary and is illustrated in **Exhibit A2-4**. MTIPS A&A accreditation boundaries contain the MTIPS SOC, MTIPS network elements, traffic scanners, event processing systems, and related systems. [redacted] The network operations center (NOC) is outside the accreditation boundaries. Connections across the accreditation boundaries include those entering the NOC and private MetTel network connections. Interconnection agreements are prepared for these systems in accordance with NIST standards and guidance. At a minimum, the MTIPS has a new

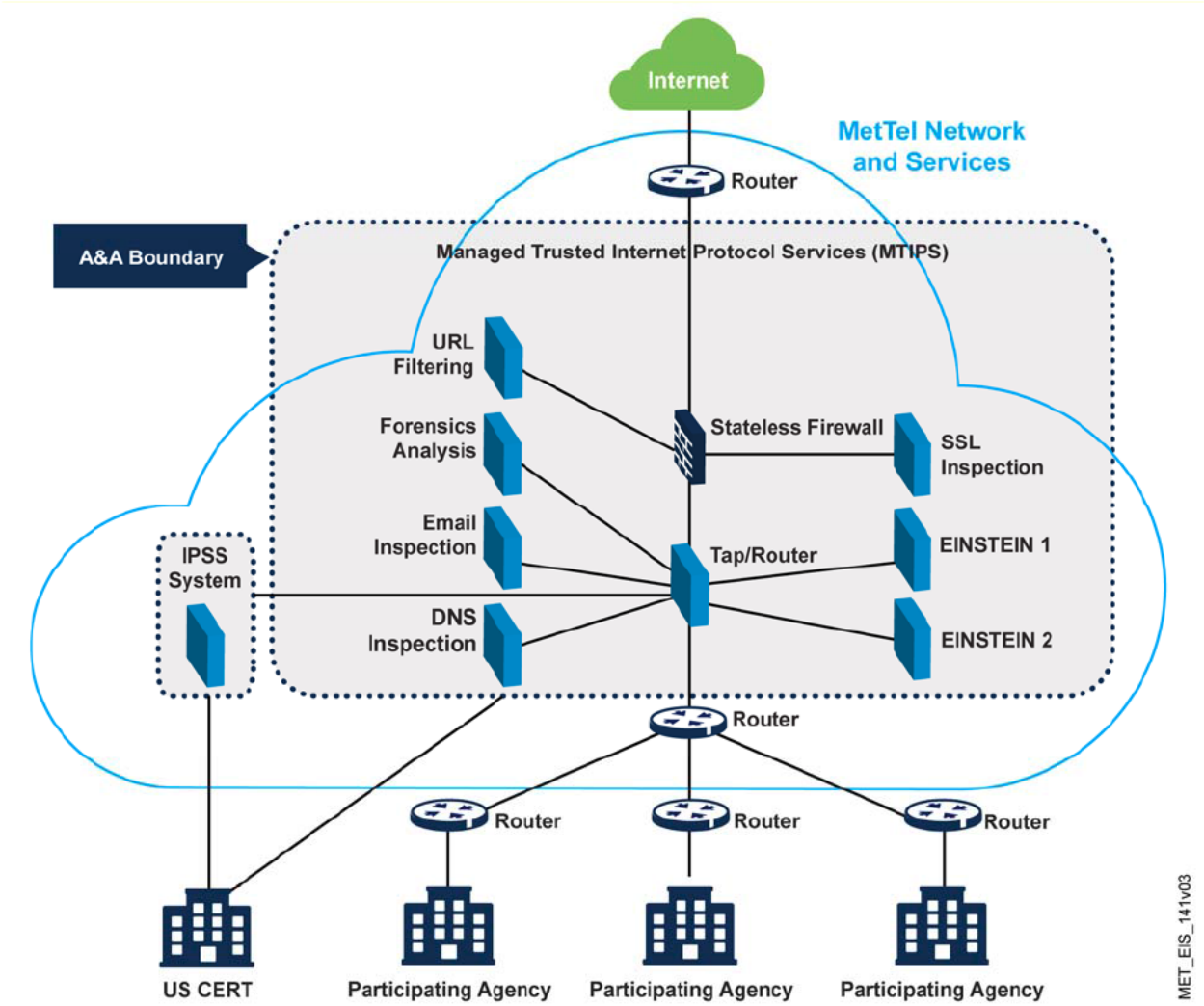


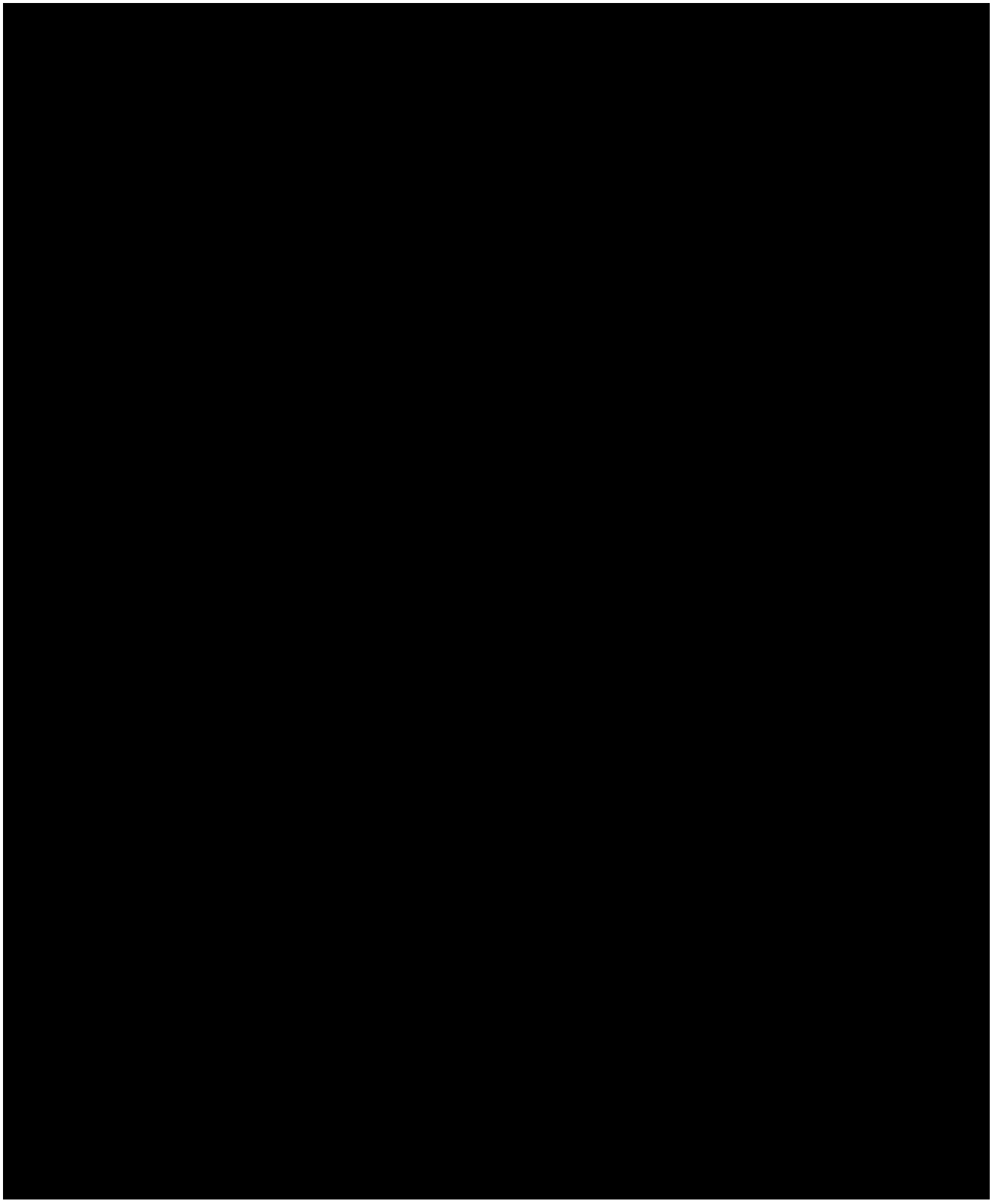
Exhibit A2-4. Assessment and Authorization Boundary and Traffic Flow

security A&A conducted and approved by GSA every 3 years or when significant change impacts the security posture of the system, as defined in NIST SP 800-37.

[redacted] The registration of the MTIPS is complete with the development of the System Security Plan (SSP). This document identifies all the security requirements of the system and describes the NIST SP 800-53 Rev 4 controls in place or planned as well as the responsibilities and expected behavior of all individuals who access the system.

[redacted]

[redacted] 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 are identified and approved, they are divided into sub-categories to identify Baseline Controls. Due to the nature of services and the protection of National Security Systems and information, classification overlays are included with additional controls required by CNSSI 1253.



Managing geographically dispersed systems is a challenge which is compounded when rapid changes are not fully documented or do not receive a thorough review. To address this, 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. The MetTel team'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

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

[redacted]

MetTel team 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, the MetTel team will ensure that mandatory configuration settings are established and implemented on

[redacted]

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 A2-9** provides an example SSP template.

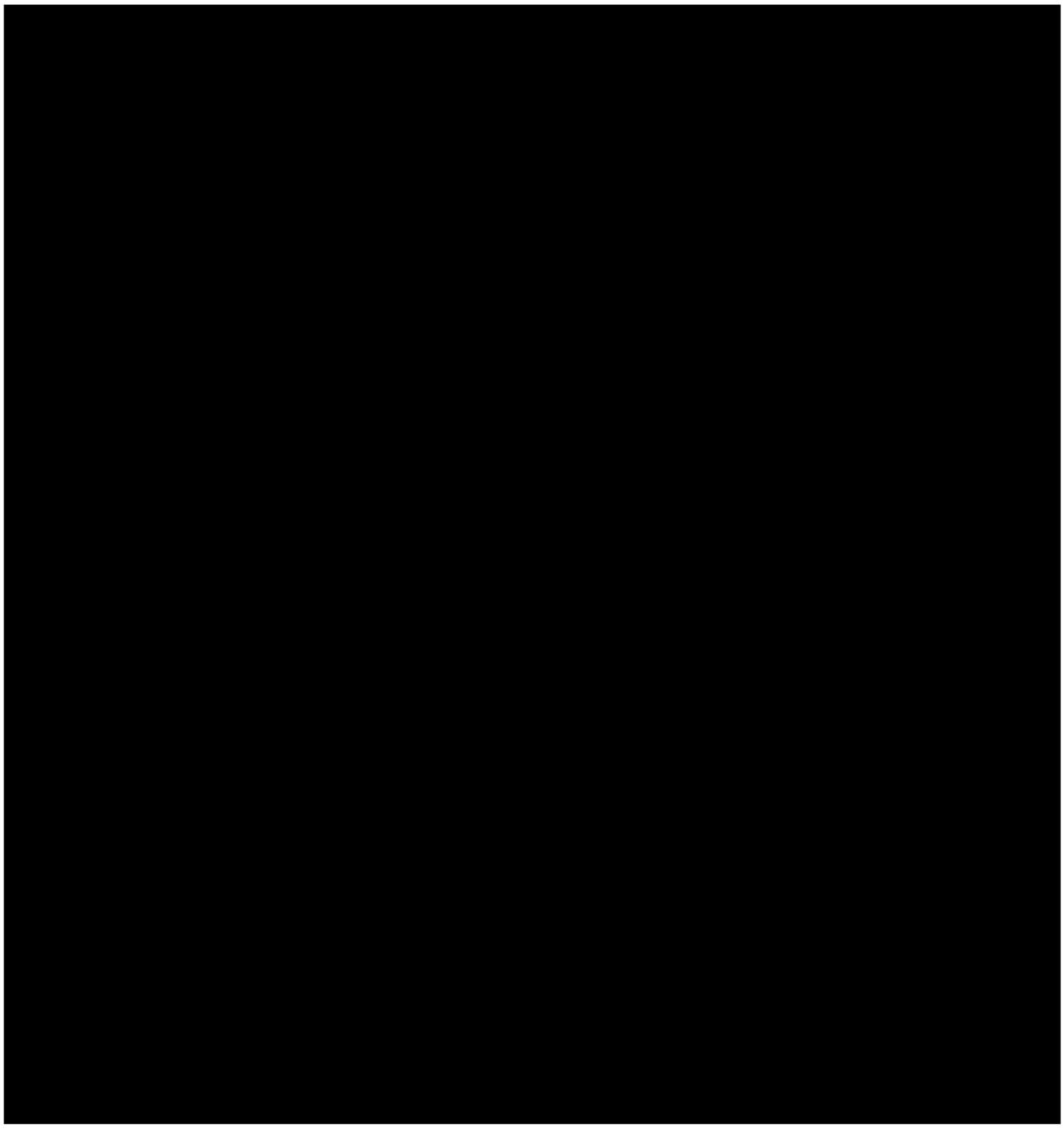


Exhibit A2-9. SSP Template Example

A2.4 STEP 4: ASSESS

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

[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.

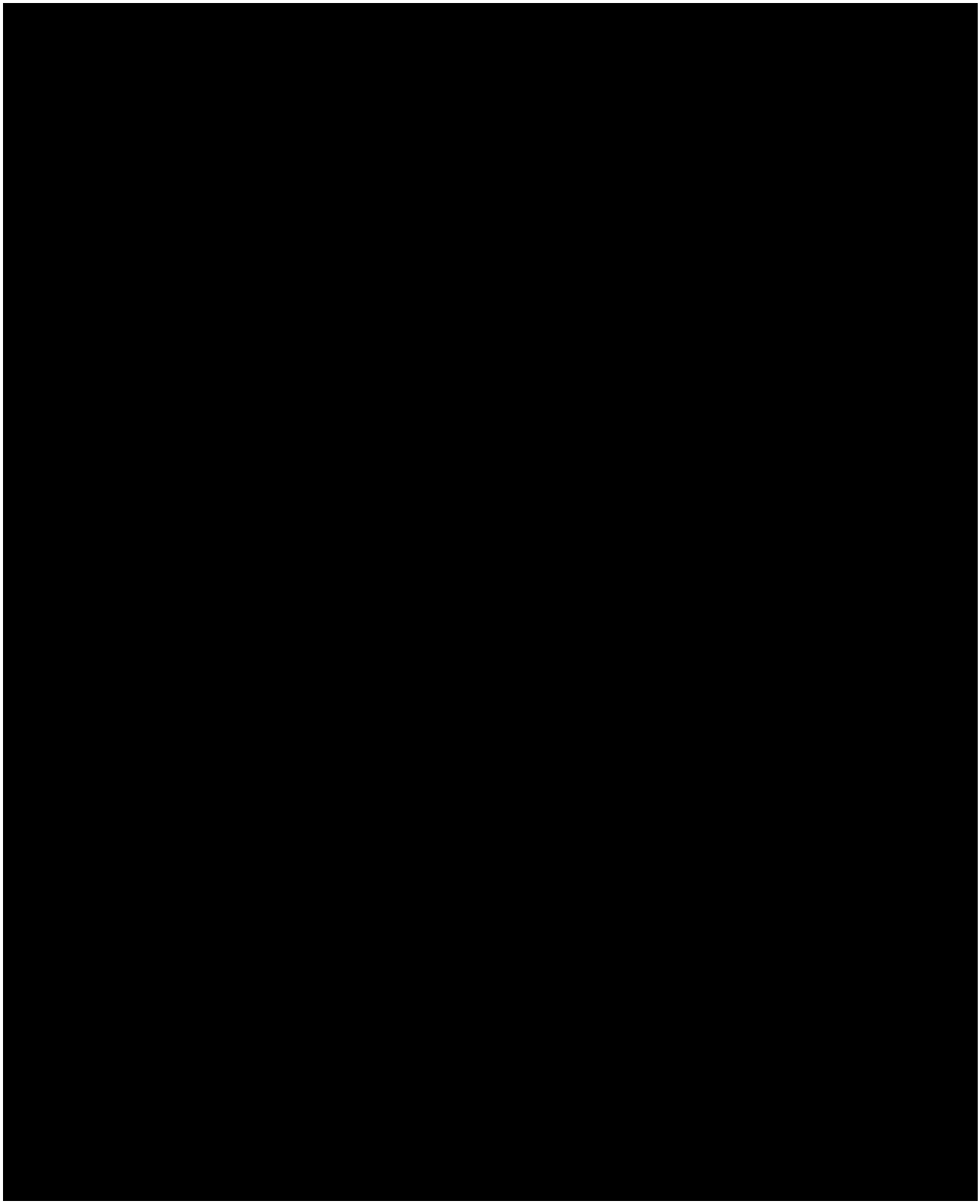


Exhibit A2-11 Example Risk Assessment Checklist

Control assessment and analysis identifies controls deemed that satisfy or do not satisfy the control objectives. This in 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***

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 A2-12**) 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

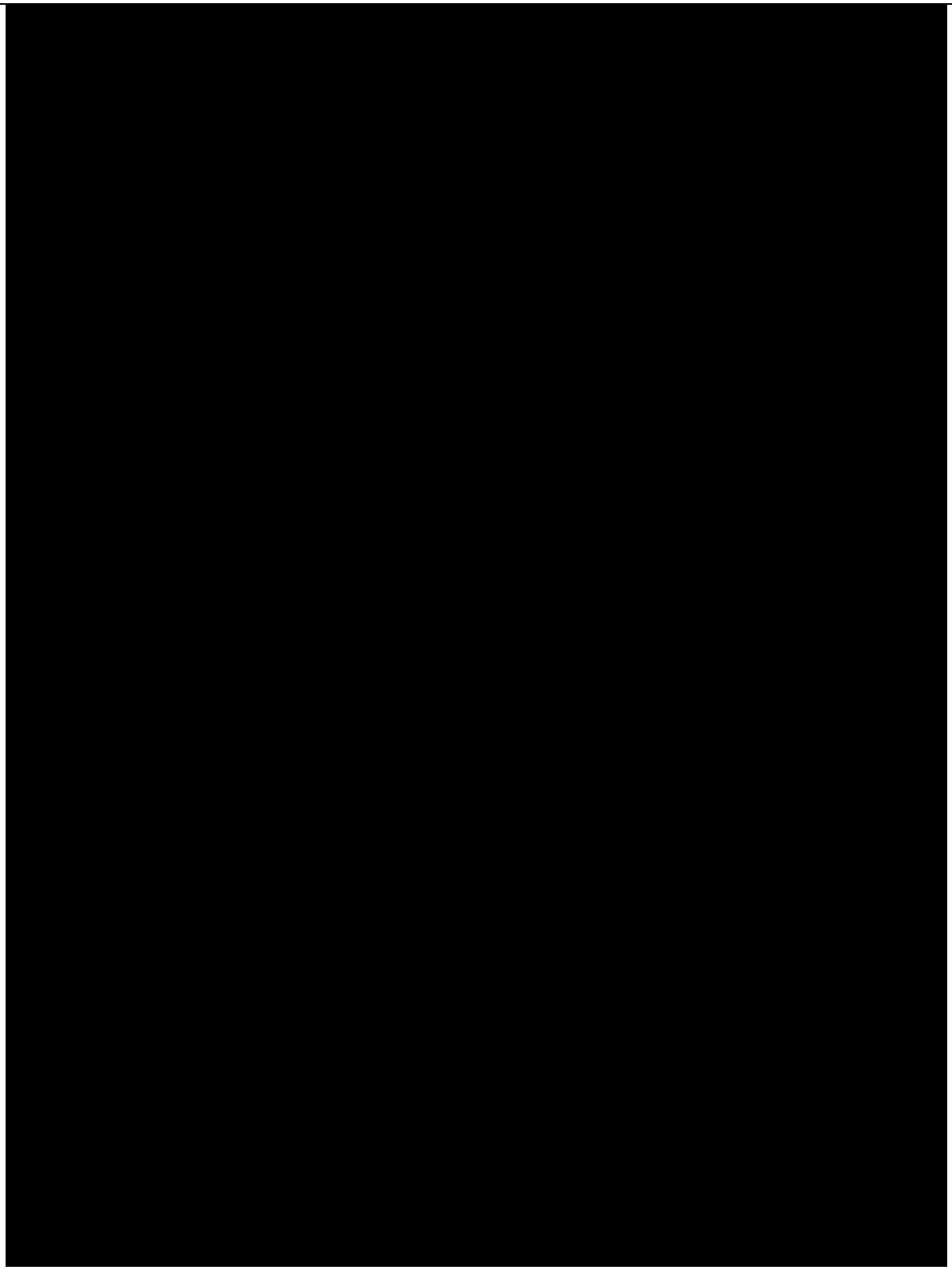


Exhibit A2-13 shows an example SAR form.

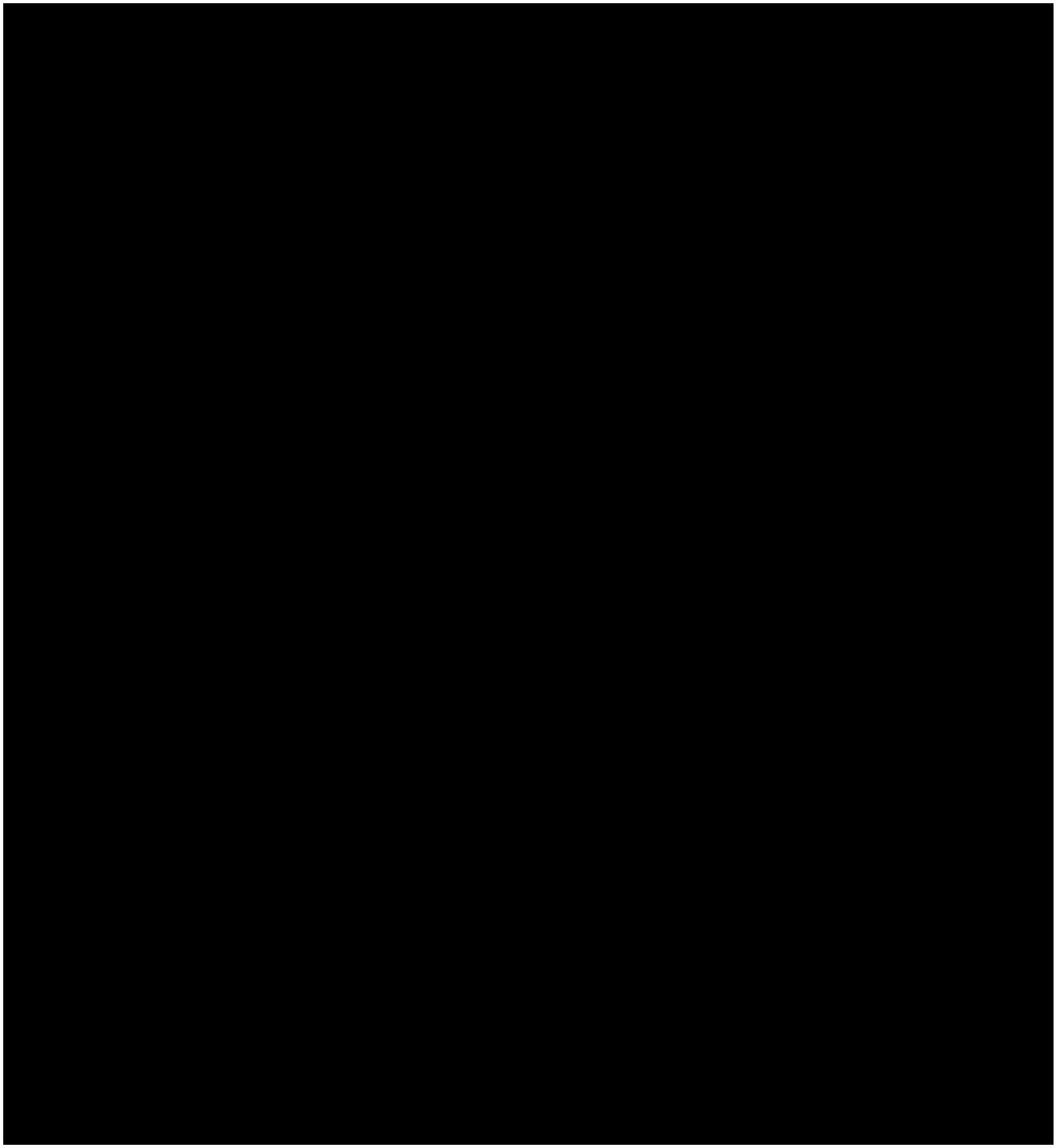


Exhibit A2-13. SAR Example

The results of the assessment and draft 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 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.

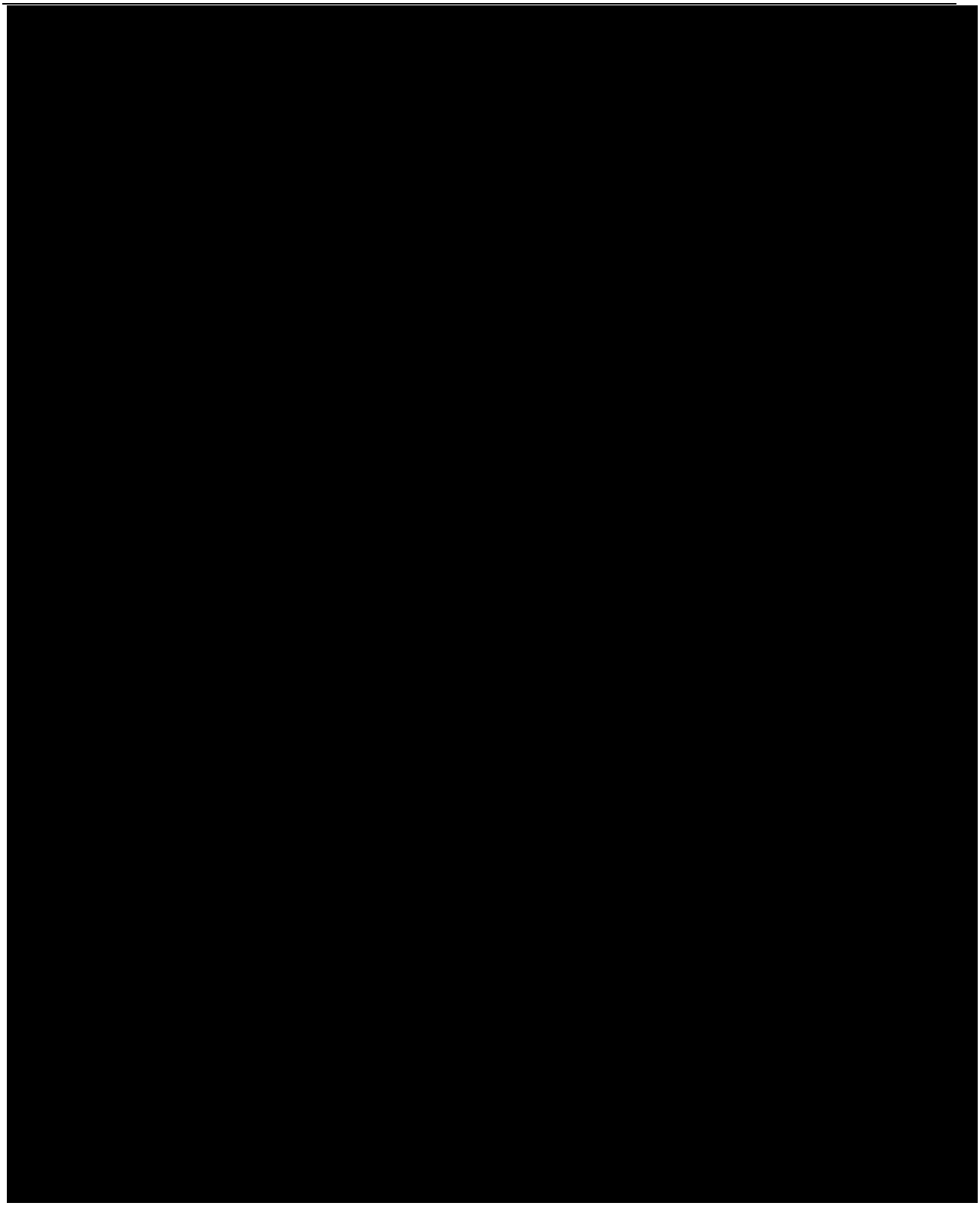
The System Owner assembles the security authorization package, which must contain at a minimum:

- 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]

[redacted]). With the technology sector continuously producing new hardware, software, and firmware, information systems are in a constant state of change. Thus, it is imperative that an effective security monitoring program 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 A2-15** illustrates how operational security contributes to continuous monitoring.



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 the MetTel team with input from the information system owner and/or common control provider and approved by the PA. For on-going security control assessments, assessors have the required degree of independence as determined by the Authorizing Official.

Exhibit A2-15. 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 PA determines the risk rating of vulnerabilities. All critical and high-risk vulnerabilities are mitigated within 30 days, and all moderate-risk vulnerabilities are mitigated within 90 days from the date the vulnerabilities are formally identified. The MetTel team updates the PA, on a monthly basis, the status of all critical and high vulnerabilities that have not been closed within 30 days. The security status of the information system (including the effectiveness of security controls employed within and inherited by the system) is reported to the Authorizing Official and other appropriate organizational officials on an on-going basis in accordance with the monitoring strategy.

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-05-24, "Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors" (Available at https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf.) • OMB Memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors" (Available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf.) • 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"

Guidance Type	Compliance Documents
	• NIST SP 800-39, "Managing Information Security Risk: Organization, Mission, and Information System View" • 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" • NIST SP 800-61 Revision 2, "Computer Security Incident Handling Guide" • NIST SP 800-64, Revision 2, "Security Consideration in the System Developments Lifecycle" • NIST SP 800-88 Revision 1, "Guidelines for Media Sanitization" • 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 800-160 "Systems Security Engineering" • NIST SP 800-161, "Supply Chain Risk Management Practices for Federal 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 Instruction 1253 (CNSSI No. 1253), Security Categorization and Control Selection for National Security Systems.
GSA Policy, Directives and Guides	• GSA Information Technology (IT) Security Policy, CIO P 2100.1(J). • GSA Order CIO P 2181.1 "GSA HSPD-12 Personal Identity Verification and Credentialing Handbook" • GSA Order CIO 2104.1, "GSA Information Technology (IT) General Rules of Behavior" • GSA CIO P 1878.1, "GSA Privacy Act Program" • GSA CIO P 1878.2A, "Conducting Privacy Impact Assessments (PIAs) in GSA" • GSA IT Security Procedural Guide 01-01, "Identification and Authentication" • GSA IT Security Procedural Guide 01-02, "Incident Response" • GSA IT Security Procedural Guide 01-05, "Configuration Management" • GSA IT Security Procedural Guide 01-07, "Access Control" • GSA IT Security Procedural Guide 01-08, "Audit and Accountability Guide" • GSA IT Security Procedural Guide 05-29, "IT Security Training and Awareness Program" • GSA IT Security Procedural Guide 06-29, "Contingency Planning" • GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk"

Guidance Type	Compliance Documents
	• GSA IT Security Procedural Guide 06-32, "Media Protection Guide" • GSA IT Security Procedural Guide 07-35, "Web Application Security Guide" • GSA IT Security Procedural Guide 08-39, "FY 2014 IT Security Program Management Implementation Plan" • GSA IT Security Procedural Guide 10-50, "Maintenance Guide" • GSA IT Security Procedural Guide 11-51, "Conducting Penetration Test Exercise Guide" • GSA IT Security Procedural Guide 12-63, "GSA's System and Information Integrity" • GSA IT Security Procedural Guide 12-64, "Physical and Environmental Protection" • GSA IT Security Procedural Guide 12-66, "Continuous Monitoring Program" • GSA IT Security Procedural Guide 12-67, "Securing Mobile Devices and Applications Guide" • GSA IT Security Procedural Guide 14-69, "SSL / TLS Implementation Guide"

APPENDIX B: NEAR-TERM DELIVERABLES AFTER AWARD

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
1	C.2.8.4.5.4	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	C.2.8.4.5.4	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	C.2.8.4.5.4	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	C.2.8.4.5.4	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	C.2.8.4.5.4	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	C.2.8.4.5.4	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	C.2.8.4.5.4	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	C.2.8.4.5.4	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	C.2.8.4.5.4	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	C.2.8.4.5.4	NIST SP 800-53 R4; CP-4	Contingency Plan Test Report (CPTR)	Initial: Within 30 days of NTP Update: Annually from contract	GSA COR/ISSO

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
				award and when significant changes occur	
11	C.2.8.4.5.4	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	C.2.8.4.5.4	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	C.2.8.4.5.4	NIST SP 800-53 R4; IR-8	Incident Response Plan (IRP)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
14	C.2.8.4.5.4	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	C.2.8.4.5.4	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	C.2.8.4.5.4	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	C.2.8.4.5.4	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	C.2.8.4.5.4	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	C.2.8.4.5.4	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

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
20	C.2.8.4.5.4	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	C.2.8.4.5.4	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	C.2.8.4.5.4	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	C.2.8.4.5.4	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