ATTACHMENT 7 BSS RISK MANAGEMENT FRAMEWORK PLAN [L.30.2.7, M.2.2.(7), G.5.6; F.2.1(41) THROUGH (76)]

A7.1 BSS SECURITY REQUIREMENTS

MetTel ensures the security of all BSS data and transactions through a layered, in depth defense security strategy which is fully compliant with all Federal regulations as listed in RFP List SECTION G.5.6.1

- Proven past performance of meeting and exceeding the security requirements of existing customer base (commercial and federal)
- Thoroughly documented security policies and procedures
- MetTel security experts provide ongoing support and guidance to ensure security and compliance with all EIS RFP requirements.

Our Business Support Systems (BSS) Risk Management Framework Plan describes how we address system security in accordance with Section G.5.6, including compliance with the Federal Information Security Management Act (FISMA) guidance and directives and all Federal regulations as listed in the RFP Section G.5.6.1. Our MetTel Federal BSS System Security Plan (SSP) supports the execution of our information security activities. Our SSP fully meets the security requirements set forth in the RFP Sections G.5.6 and includes specific procedures for how to execute the plan.

MetTel's BSS SSP is based on the NIST FIPS-199 categorization of Moderate Impact, per the RFP requirement in G.5.6. We have selected and implemented the appropriate controls for Moderate Impact systems from each of the Control Families, as specified in NIST SP 800-53 Rev.4. We will fully cooperate with the Government and provide all required documentation to verify that these standards and practices are being met.

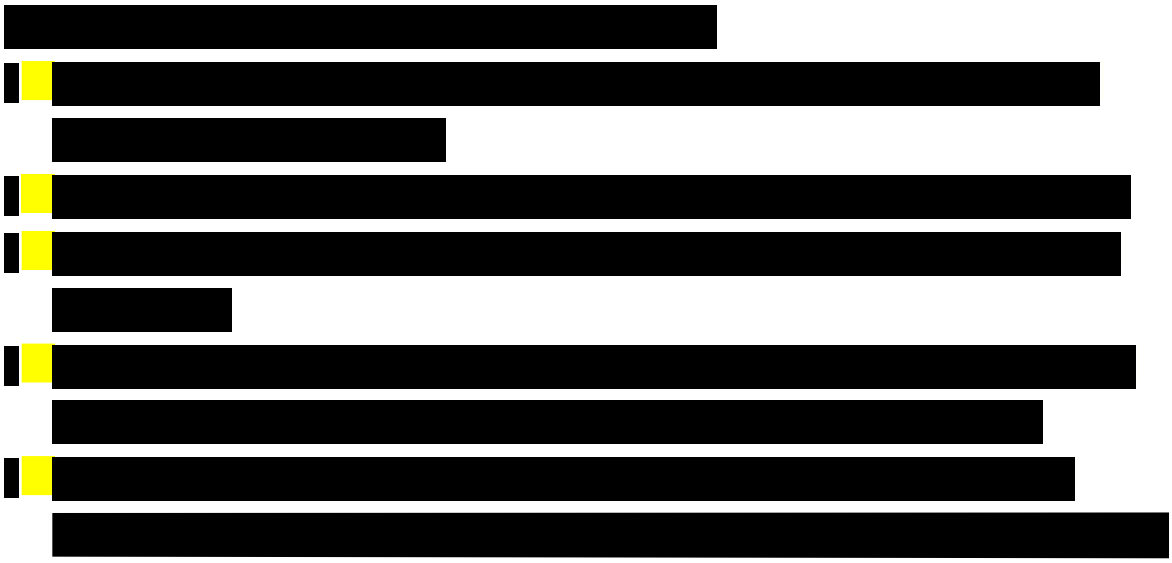


Exhibit A7-1. Post-Award Deliverables

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
41	G.5.6.4	NIST SP 800-53 R4; CA-5 NIST SP 800-53 R4; RA-5	Plan of Action and Milestones (POA&M) Vulnerability scanning reports for Operating System, Web Application, and Database scans (as applicable)	Initial: With the Security A&A package Update: Quarterly	GSA COR/ISSO
42	G.5.6.4	NIST SP 800-53 R4; PL-2	BSS System Security Plan (SSP)	Initial: Within 30 days of NTP Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
43	G.5.6.4	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
44	G.5.6.4	NIST SP 800-53 R4; CA-3	Information System Interconnection Security Agreements (ISA)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
45	G.5.6.4	NIST SP 800-53 R4; AC-1	GSA NIST 800-53 R4 Control Tailoring Workbook	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
46	G.5.6.4	NIST SP 800-53 R4; AC-1	GSA NIST SP 800-53 R4 Control Summary Table	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
47	G.5.6.4	NIST SP 800-53 R4; PL-4	Rules of Behavior (RoB)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur.	GSA COR/ISSO
48	G.5.6.4	NIST SP 800-53 R4; CM-8	System Inventory	Initial: With the Security A&A package Update: Annually from	GSA COR/ISSO

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
				contract award and when significant changes occur	
49	G.5.6.4	NIST SP 800-53 R4; CP-2	Contingency Plan (CP)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
50	G.5.6.4	NIST SP 800-53 R4; CP-4	Contingency Plan Test Plan (CPTP)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
51	G.5.6.4	NIST SP 800-53 R4; CP-4	Contingency Plan Test Report (CPTR)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
52	G.5.6.4	NIST SP 800-53 R4; AR-2, AR-3 and AR-4	Privacy Impact Assessment (PIA)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
53	G.5.6.4	NIST SP 800-53 R4; CM-9	Configuration Management Plan (CMP)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
54	G.5.6.4	NIST SP 800-53 R4; IR-8	Incident Response Plan (IRP)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
55	G.5.6.4	NIST SP 800-53 R4; IR-3	Incident Response Test Report (IRTR)	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
56	G.5.6.4	NIST SP 800-53 R4; CA-7	Continuous Monitoring Plan	Initial: With the Security A&A package Update: Annually from contract award and when significant changes occur	GSA COR/ISSO

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
57	G.5.6.4	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
58	G.5.6.4	NIST SP 800-53 R4; SA-11	Code Review Report (If applicable)	Initial: Prior to placing the information system into production Update: Annually from contract award and when significant changes occur	GSA COR/ISSO
59	G.5.6.4	NIST SP 800-53 R4; CA-2	Annual FISMA Assessment	Annually from contract award	GSA COR/ISSO
60	G.5.6.4	NIST SP 800-53 R4; AC-1	Access Control Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
61	G.5.6.4	NIST SP 800-53 R4; AT-1	Security Awareness and Training Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
62	G.5.6.4	NIST SP 800-53 R4; AU-1	Audit and Accountability Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
63	G.5.6.4	NIST SP 800-53 R4; CA-1	Security Assessment and Authorization Policies and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
64	G.5.6.4	NIST SP 800-53 R4; CM-1	Configuration and Management Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
65	G.5.6.4	NIST SP 800-53 R4; CP-1	Contingency Planning Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
66	G.5.6.4	NIST SP 800-53 R4; IA-1	Identification and Authentication Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO

ID	Requirement Reference	Deliverable Description Reference	Deliverable Name	Frequency	Deliver To
67	G.5.6.4	NIST SP 800-53 R4; IR-1	Incident Response Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
68	G.5.6.4	NIST SP 800-53 R4; MA-1	System Maintenance Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
69	G.5.6.4	NIST SP 800-53 R4; MP-1	Media Protection Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
70	G.5.6.4	NIST SP 800-53 R4; PE-1	Physical and Environmental Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
71	G.5.6.4	NIST SP 800-53 R4; PL-1	Security Planning Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
72	G.5.6.4	NIST SP 800-53 R4; PS-1	Personnel Security Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
73	G.5.6.4	NIST SP 800-53 R4; RA-1	Risk Assessment Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
74	G.5.6.4	NIST SP 800-53 R4; SA-1	Systems and Services Acquisition Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
75	G.5.6.4	NIST SP 800-53 R4; SC-1	System and Communication Protection Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO
76	G.5.6.4	NIST SP 800-53 R4; SI-1	System and Information Integrity Policy and Procedures	Initial: Reviewed during Security A&A Update: Biennially from contract award	GSA COR/ISSO

We use a comprehensive “layered, defense in depth” methodology to protect our Federal BSS. **Exhibit A7-2** depicts the components of our methodology.

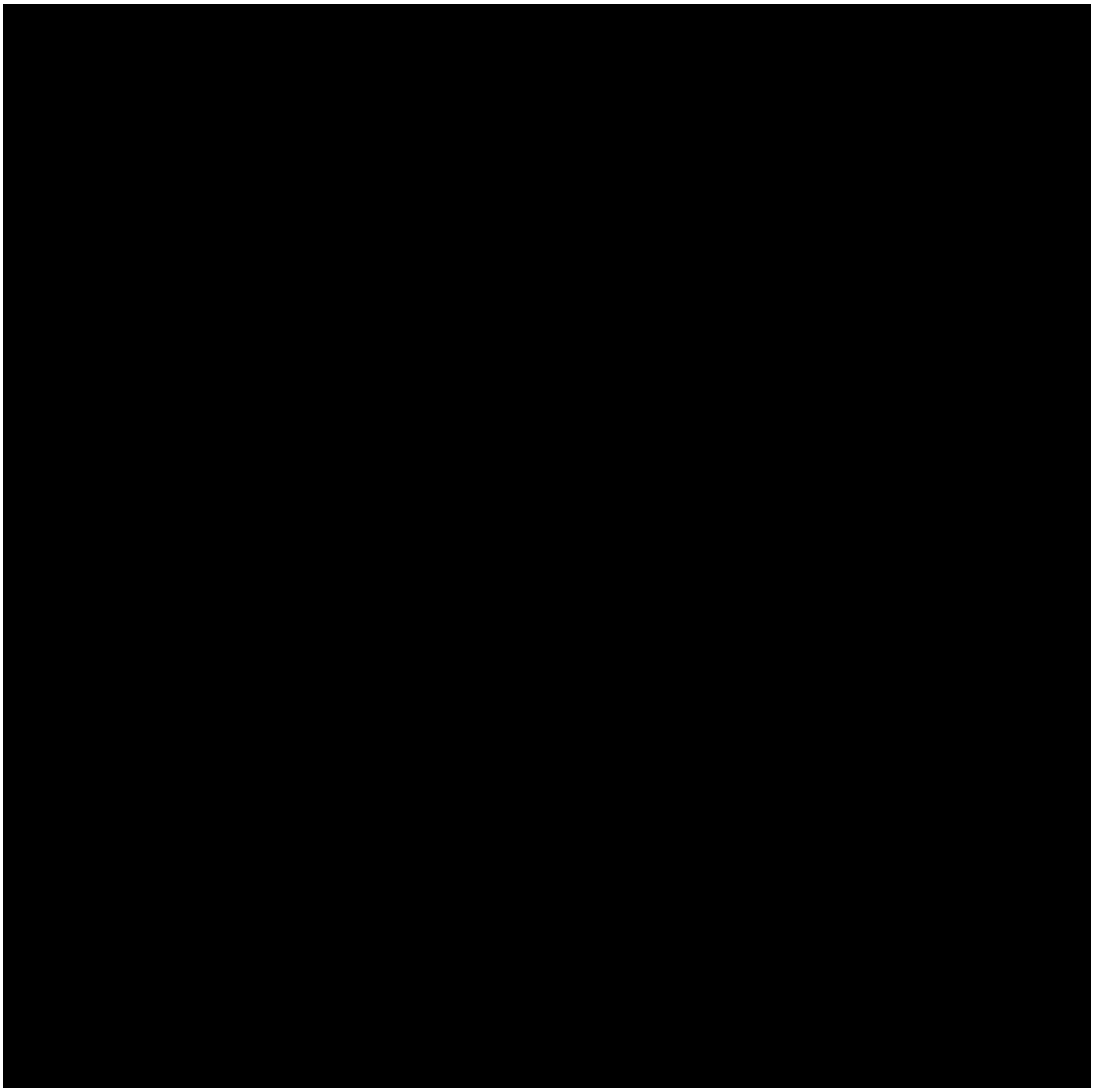


Exhibit A7-2. MetTel’s Layers of Defense

[redacted]

In addition to the combined layered in depth approach, we apply the National Institute of Standards and Technology (NIST) Risk Management Framework (**Exhibit A7-3**) to the management of our MetTel Federal BSS and our written and security policies and procedures. We manage risk through structured, yet flexible, sets of activities categorized into six steps: 1) Categorize, 2) Select, 3) Implement, 4) Assess, 5) Authorize, and 6) Monitor. These six steps (see **Exhibits A7-4** through **A7-9**), required by the Risk Management Framework, enable us to conduct day-to-day operations in support of GSA and Agency users, protect information and make informed risk decisions as we implement, enhance and maintain MetTel's Federal BSS.

Exhibit A7-3. Risk Management Framework Overview

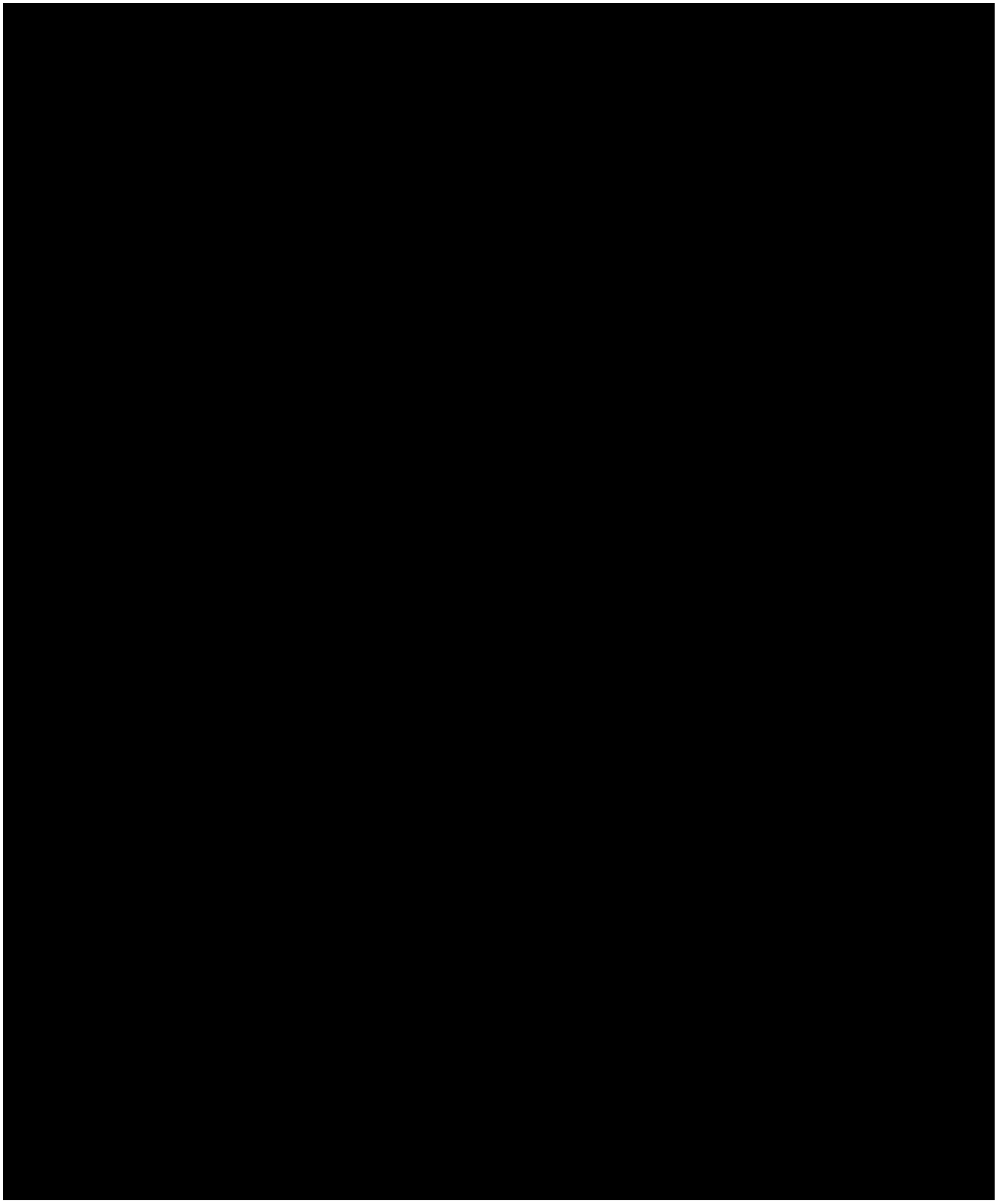


Exhibit A7-4. The Categorize Step

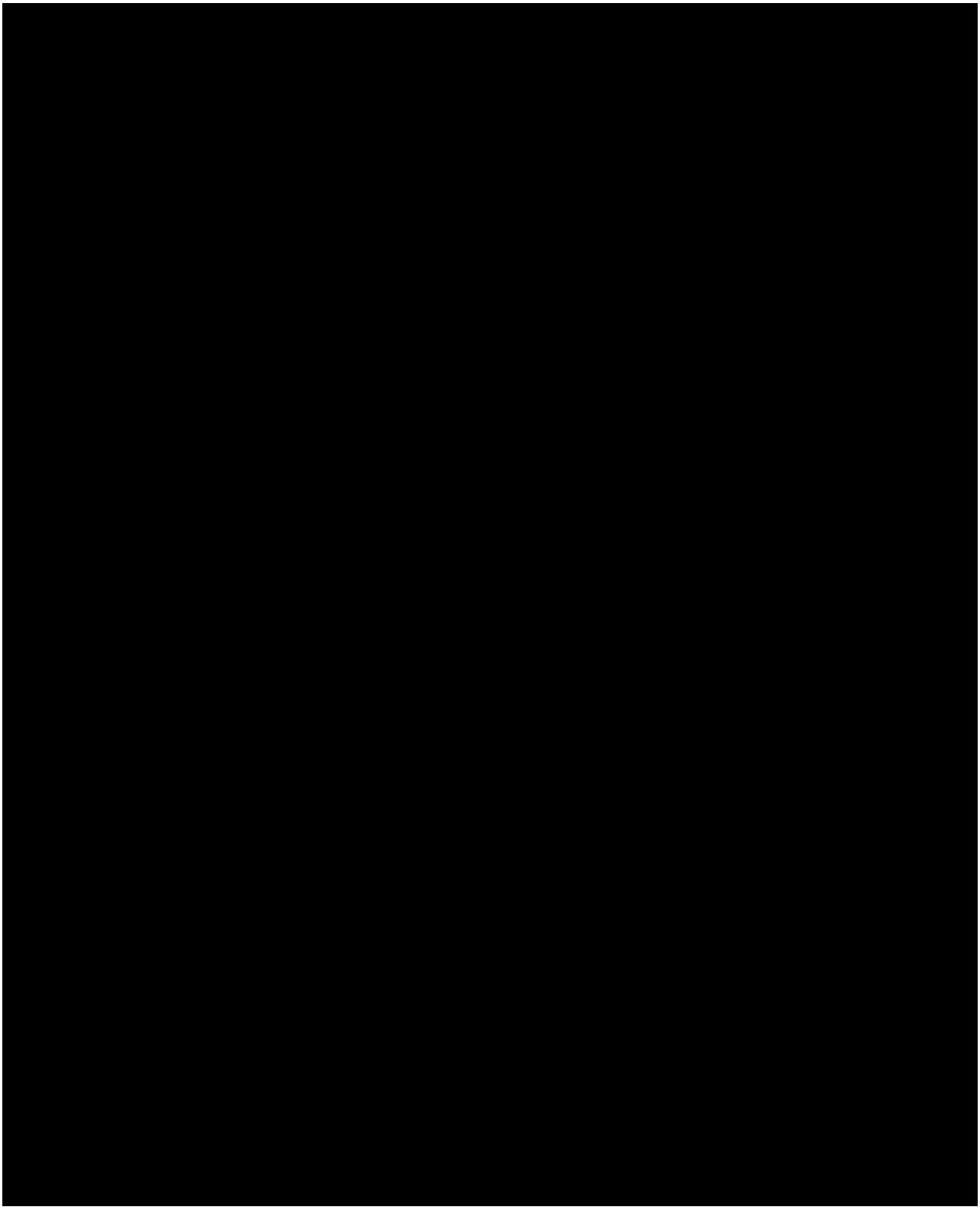


Exhibit A7-5. The Select Step

Exhibit A7-6. The Implement Step

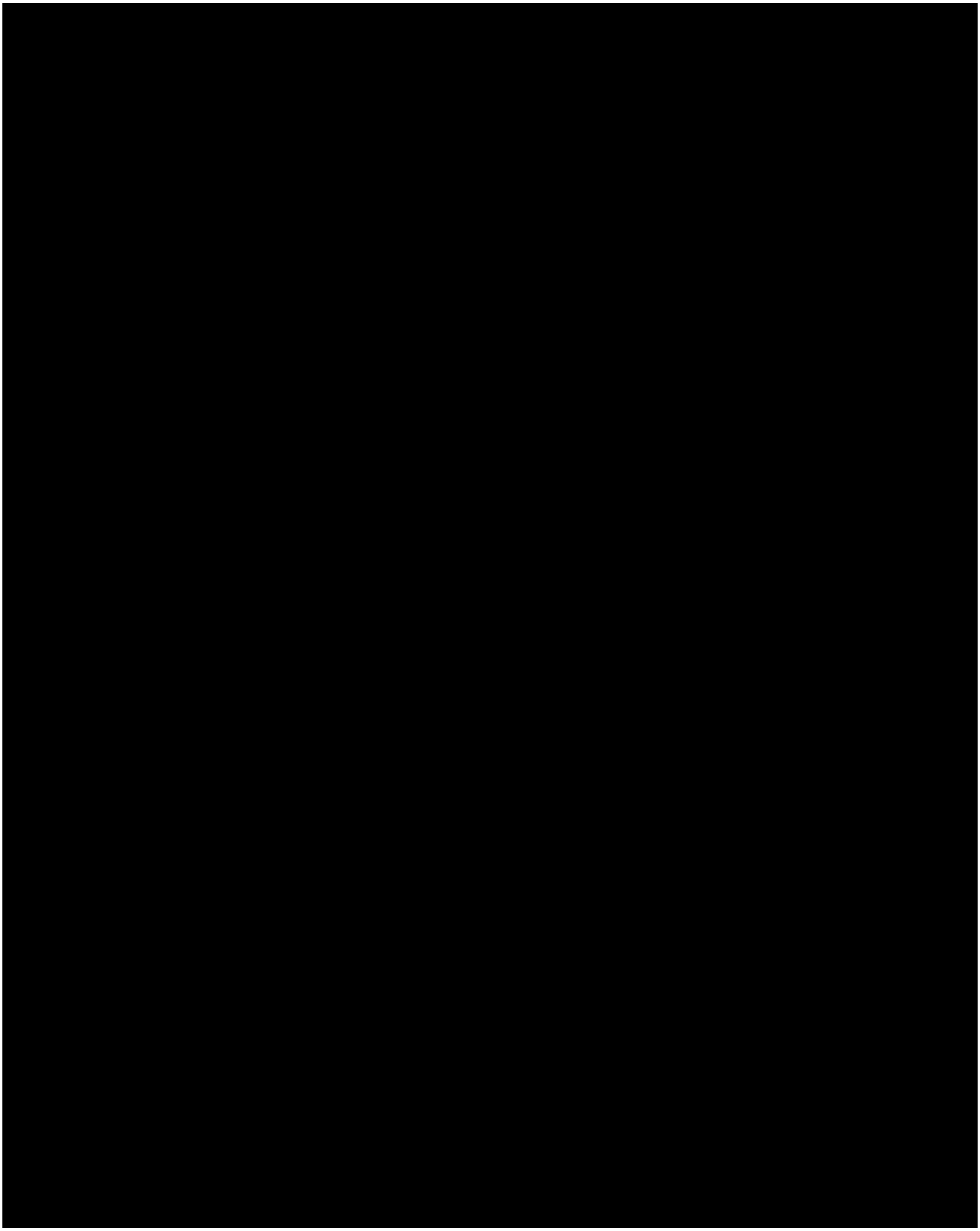


Exhibit A7-7. The Assess Step

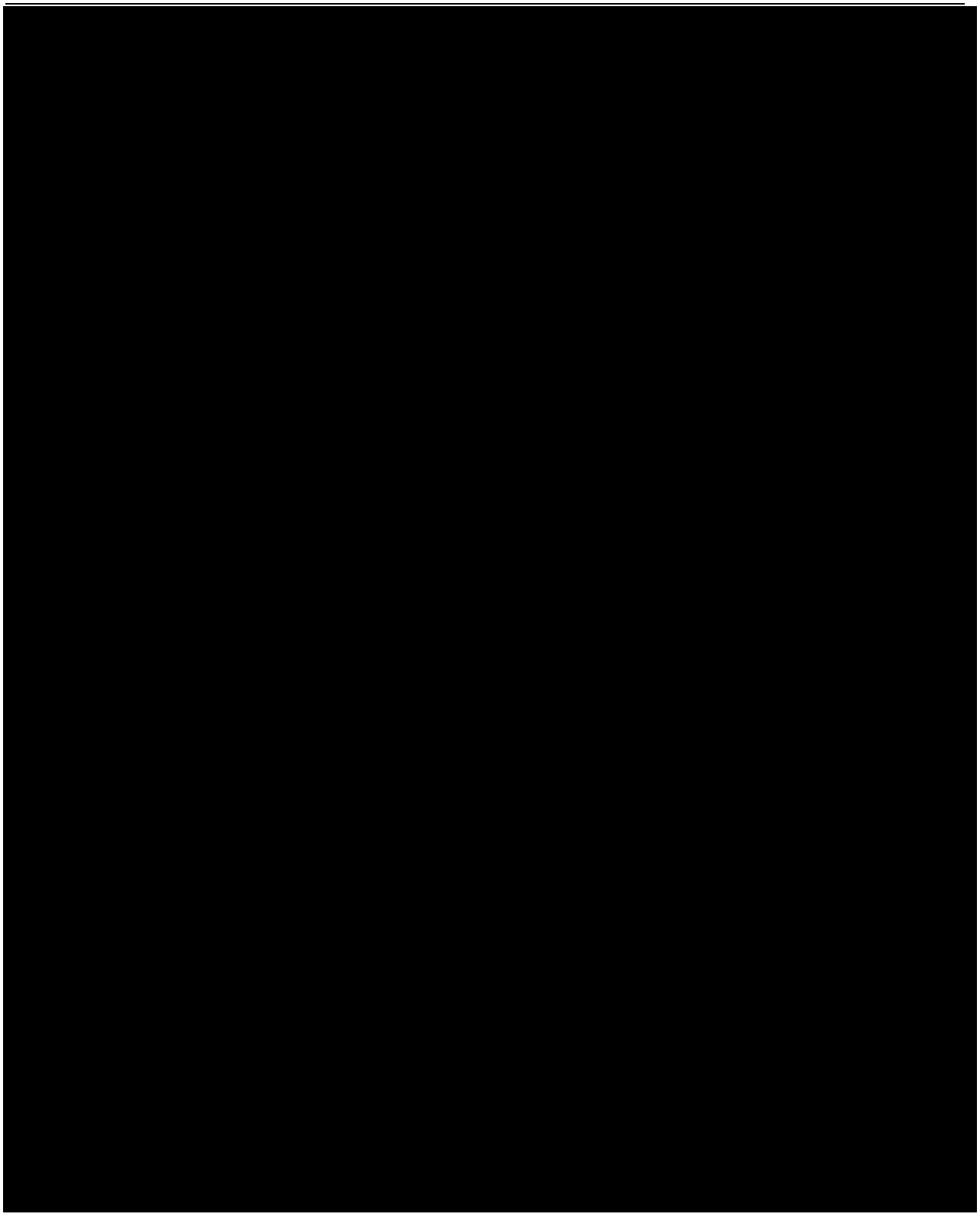


Exhibit A7-8. The Authorize Step

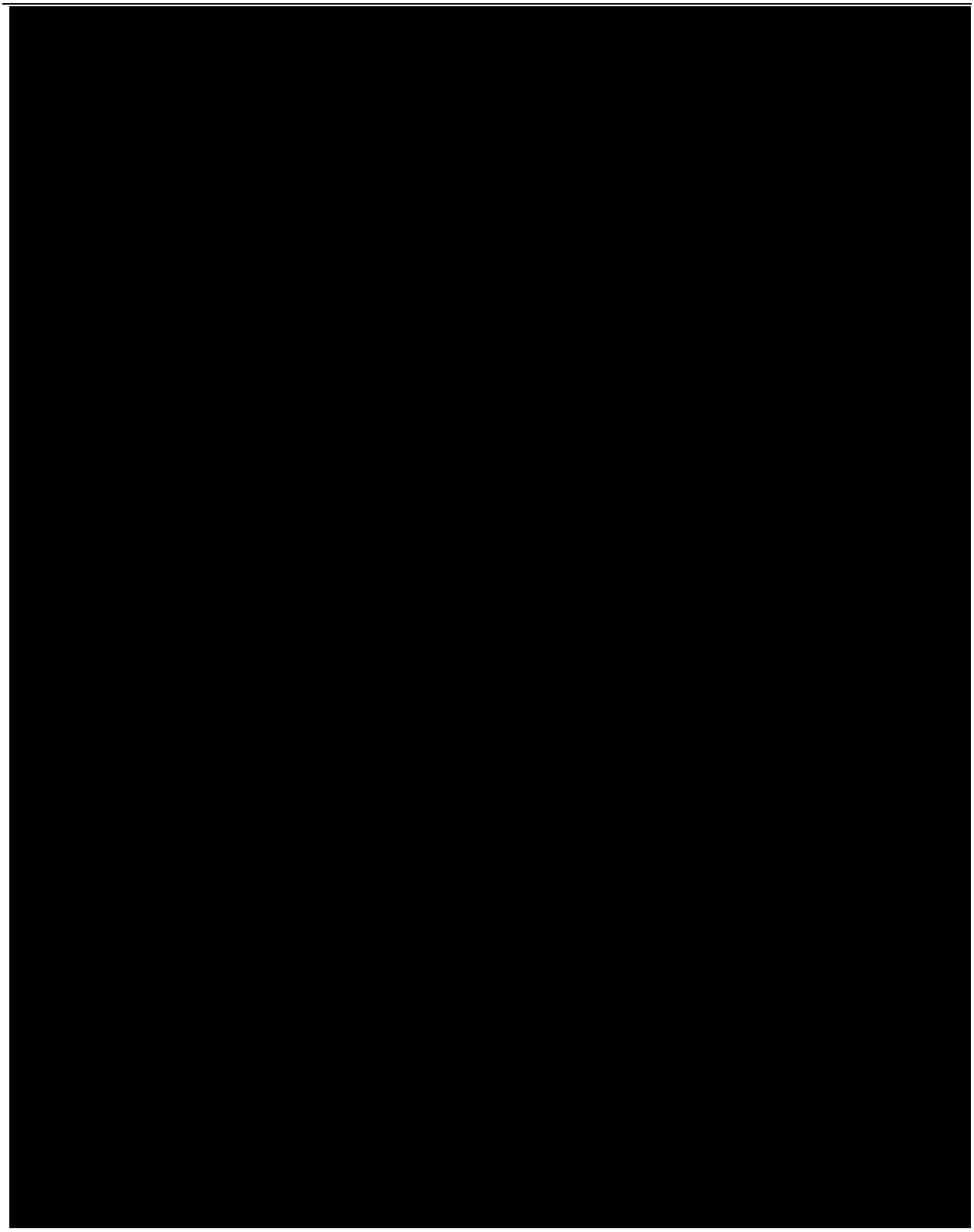


Exhibit A7-9. The Monitor Step

Exhibit A7-10 summarizes how we apply the NIST Risk Management Framework to MetTel's Federal BSS.

Exhibit A7-10. MetTel's Security Lifecycle

Policies, Procedures and Awareness:

To support our Security Lifecycle and protect the MetTel Federal BSS from unauthorized access, use, disclosure, disruption, modification or destruction of information, we developed a BSS SSP and a comprehensive set of [redacted] MetTel security policies and procedures. All policies and procedures are based on the NIST SP 800 and FIPS series of guidance, and include, but are not limited to:

[redacted]

Training is a mission critical component of our security methodology. We have a rigorous awareness and training program, including a Security Awareness and Training Plan, to ensure that our Federal BSS staff is well versed in our security policies, plans and procedures; participates in exercises to practice the execution of procedures; and is well equipped to operate in today's complex cyber-threat environment.

[redacted]

Internal Network:

The single greatest threat to MetTel's Federal BSS internal network is that of insider threat. We work to counter insider threats by enhanced background examinations of our staff members and by following the federal background investigation protocol specified in the GSA EIS RFP. We apply the principal of role-based access so that only those

MetTel staff members who have a verified need for access to our Federal BSS are granted such access. [redacted]

Host:

[redacted]

Applications:

[redacted]

- Customer Portal
- Provisioning
- Billing
- Pricing and Service Catalog
- Reporting

[redacted]

Data:

[redacted]

A7.1.1 General Security Compliance Requirements

We fully comply with all current applicable and federal agency-specific IT security directives as listed in G.5.6.1, standards, policies and reporting requirements. MetTel fully complies with the Federal Information Management Security Act (FISMA) guidance and directives to include Federal Information Processing Standards (FIPS), the NIST Special Publication (SP) 800 series guidelines, GSA IT security directives, policies and guides, and other applicable Government-wide laws and regulations for the protection and security of Government IT. Our compliance includes, but is not limited to, the documents in G.5.6.1.

A7.1.2 GSA Security Compliance Requirements

MetTel's Federal BSS is categorized at the Moderate Impact Level based on the criteria specified in FIPS 199 and FIPS 200. We developed our Federal BSS Risk Management Framework Plan in accordance with the guidance set forth in NISP SP 800-37 and the requirements of the GSA EIS RFP. **Exhibit A7-11** (page 2-A7-28) is a draft of our **MetTel Systems Security Compliance Policy** and it describes our approach for BSS security compliance at the Moderate Impact level.

A7.1.3 Security Assessment and Authorization (Security A&A)

MetTel acknowledges that our Federal BSS must pass a valid security A&A prior to being placed into operation and processing Government information. MetTel will maintain a valid security A&A. MetTel fully understands that failure to do so will be grounds for termination of the contract. MetTel agrees that our Federal BSS must undergo a new security A&A at least every three (3) years, or when there is a significant change that impacts our systems security posture.

A7.1.4 BSS System Security Plan (BSS SSP)

We meet all Federal security A&A requirements, as mandated by federal laws, directives and policies, and will make available any documentation, physical access, and logical access needed to support this requirement. When the GSA PMO requests the related documentation, we will make this documentation immediately available to the GSA PMO. Our security A&A is based on BSS's NIST FIPS- 199 categorization of Moderate Impact.

We assert that our MetTel Federal BSS SSP is in accordance with NIST SP 800-18 and NIST SP 800-53 Rev4. We will complete and submit a final BSS SSP to the GSA COR/ISSO within 30 days of the Notice to Proceed (NTP) to include annual updates.

MetTel is required to, and will, create, maintain, and update the following A&A documentation:

1. We have developed and maintain a Security Assessment Boundary and Scope Document (BSD) as identified in NIST SP 800-37. We will complete our BSD and submit within 15 days of NTP, to include annual updates.

2. We developed and maintain Interconnection Security Agreements (ISA) in accordance with NIST SP 800-47. We will provide any existing ISA's with our initial security A&A package and will include annual updates.
3. We developed and maintain a GSA Control Tailoring Workbook as identified in GSA Security Procedural Guide 06-30, "Managing Enterprise Risk". We documented all MetTel implemented settings, which differ from GSA's settings. We developed a Control Tailoring Workbook for the MetTel BSS to be included with our initial security A&A package and to include annual updates.
4. We developed and maintain a GSA Control Summary Table for a Moderate Impact Baseline as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk." We developed a GSA NIST SP 800-53 R4 Control Summary Table for our Federal BSS to include with our initial security A&A package, and to include annual updates.
5. We developed, implemented and maintain Rules of Behavior (RoB) for our Federal BSS users as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk" and GSA Order CIO 2104.1, "GSA IT General Rules of Behavior." We will provide our RoB for our Federal BSS with our initial security A&A package, to include annual updates.
6. We developed and maintain a System Inventory that includes hardware, software and related information as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk." We will provide a System Inventory for our Federal BSS with our initial security A&A package, to include annual updates.
7. We developed and maintain a Contingency Plan (CP), including Disaster Recovery Plan (DRP) and Business Impact Assessment (BIA) completed in compliance with NIST SP 800-34. We will provide a CP, DRP, and BIA for our Federal BSS with our initial security A&A package, to include annual updates.
8. We developed and maintain a Contingency Plan Test Plan (CPTP) completed in compliance with GSA IT Security Procedural Guide 06-29, "Contingency Planning Guide." We will provide a CPTP for our Federal BSS with our initial security A&A package, to include annual updates.

9. We tested our Contingency Plan and documented the results in a Contingency Plan Test Report (CPTR), in compliance with GSA IT Security Procedural Guide 06-29, “Contingency Planning Guide.” We will provide a CPTR for our Federal BSS with our initial security A&A package, to include annual updates.
10. We performed and completed a Privacy Impact Assessment (PIA) as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.” We will provide our PIA for our Federal BSS with our initial security A&A package, to include annual updates.
11. We developed and maintain a Configuration Management Plan (CMP). Further, we will provide a CMP for our Federal BSS with our initial security A&A package, to include annual updates.
12. MetTel developed and maintains a System Baseline Configuration Standard Document. We will provide a well-defined, documented Baseline Configuration, and up-to-date specification to which our Federal BSS is built. We will provide the System Baseline Configuration for our Federal BSS as a part of the CMP and submit it with our initial security A&A package, to include annual updates.
13. We developed and maintain an accurate System Configuration Settings for our Federal BSS. We established and documented the mandatory configuration settings for information technology products employed within our Federal BSS that reflect the most restrictive mode consistent with BSS operational requirements. We configured our Federal BSS in accordance with GSA technical guides, NIST standards, Center for Internet Security (CIS) guidelines (Level 1), and/or industry best practices in hardening our BSS and will do so as deemed appropriate by the AO. These settings are included as part of our Configuration Management plan which we will update and/or review on an annual basis.
14. We developed and maintain an Incident Response Plan (IRP). We will provide the IRP to our Federal BSS with our initial security A&A package, to include annual updates.
15. We tested the IRP and documented the results in an Incident Response Test Report (IRTR). We will provide the IRTR for our Federal BSS with our initial security A&A package, to include annual updates.

16. We developed and maintain a Continuous Monitoring Plan, documenting how the monitoring of our Federal BSS is accomplished. MetTel has exercised and will do so in the future, our Continuous Monitoring Plan. The Plan provides our current understanding of the security state and risk posture of the information systems. We will update and submit the security controls and supporting deliverables to GSA, per the mandated schedule. We will provide a Continuous Monitoring Plan for our Federal BSS with our initial security A&A package, which will be updated annually.
17. We develop and maintain a Plan of Action and Milestones (POA&M), completed in compliance with GSA IT Security Procedural Guide 06-30, “Plan of Action and Milestones.” All of MetTel’s scans, documentation and update reports associated with the POA&M will be performed as an “authenticated user role” with elevated privileges. MetTel documented all vulnerability scanning results to date. We will integrate these scans into the POA&M and submit together with our quarterly POA&M. We will include all scans for all networking and computing components which are within our Federal BSS security accreditation boundary. We will submit all appropriate vulnerability scans with our initial security A&A package and ensure that an annual BSS User Certification/Authorization Review is annotated within the POA&M. We will provide our POA&M based on our Security Testing and Evaluation (ST&E) process for our Federal BSS as part of our initial security A&A package, followed by quarterly updates.
18. MetTel’s BSS, has been categorized by FIPS-199 as Moderate Impact BSS, and is subjected to a completed independent internal and external penetration tested by our scanning vendor “E-Plus, Inc.” MetTel will provide an Independent Penetration Test Report, documenting the results of the vulnerability analysis and exploitability of identified vulnerabilities with our A&A boundary. On an annual basis in accordance with GSA CIO-IT Security Guide 11-51, we will follow GSA instructions, regarding the scheduling and performance of these penetration exercises. We will coordinate all penetration test exercises through the GSA Office of the Chief Information Security Officer (OSISO) Security Engineering (ISE) division at itsecurity@gsa.gov per GSA CIO-IT Security Guide 11-51.

19. Because the MetTel Federal BSS meets the requirements of FIPS 199 Moderate Impact BSS, we perform automated code analysis reviews in accordance with GSA CIO Security Procedural Guide 12-66, [redacted] and document those results in a Code Review Report that we submit prior to placing our Federal BSS into production, when there are changes to code and on an annual basis.
20. We will allow GSA employees (or GSA-designated third-party contractors) to conduct security A&A activities, to include control reviews in accordance with NIST SP 800-53 R4 / NIST SP 800-53A R4 and GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk." We agree that review activities include, but are not limited to, operating system vulnerability scanning, web application scanning, and database scanning of applicable BSS components that support the processing, transportation, storage, or security of Government information. We will fully cooperate with Government representatives in the performance of these tests. We agree that our Federal BSS infrastructure scans will performed as an authenticated user with elevated privileges.
21. We currently track all identified gaps between the required 800-53 R4 controls and MetTel's BSS implementation as documented in the Security/Risk Assessment Report (SAR) for mitigation in a POA&M document, to be completed by us in accordance with GSA IT Security Procedural Guide 06-30 "Managing Enterprise Risk".
22. We will mitigate and fully document all security risks found during the security A&A and continuous monitoring activities. We agree to mitigate all critical and high-risk vulnerabilities within 30 days and all moderate risk vulnerabilities will be mitigated within 90 days from the date vulnerabilities are formally identified. We agree that the Government will determine the risk rating of vulnerabilities. We will provide monthly updates on the status of all critical and high vulnerabilities that have not been closed within 30 days.
23. We will deliver the results of our annual FISMA assessment conducted per GSA CIO IT Security Procedural Guide 04-26, "FISMA Implementation." We will, each

fiscal year, complete an annual assessment, in accordance with instructions provided by GSA.

24. We have developed and keep current all policy and procedures documents, as outlined in the specified NIST documents, as well as appropriate GSA IT Security Procedural Guides. We agree that the list of documents in G.5.6.4 – 24 must be verified and reviewed during our initial Security Test and Evaluation assessment (ST&E) with updates provided to the GSA COR/ISSO/ISSM biennially.

A7.1.5 Additional Security Requirements

We will adhere to the proper privacy and security safeguards, in accordance with the FAR Part. 52.239-1. We will properly label deliverables identified in Section C.5.6.6 as "CONTROLLED UNCLASSIFIED INFORMATION" (CUI document sensitivity). We agree to ensure that external transmission/dissemination of Controlled Unclassified Information (CUI) data to and/or from a Federal computer are encrypted. Certified encryption modules must be encrypted and certified encryption modules must be used in accordance with FIPS PUB 140-2, "Security Requirements for Cryptographic Modules." We use SSL to secure transactions between Federal customers and our Federal BSS. All our SSL certificates are purchased from DigiCert and are completely up to date. Copies of our SSL certificates will be presented to the Government upon request. Where appropriate, we will ensure implementation of the requirements identified in the FAR 52.224-1 "Privacy Act Notification" and FAR 52.224-2 "Privacy Act".

We will cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal Government's agent.

We acknowledge that the Government has the right to preform manual and/or automated audits, scans, reviews, or other inspections of MetTel's BSS IT environment being used to provide and/or facilitate services for the Government, in accordance with the FAR.

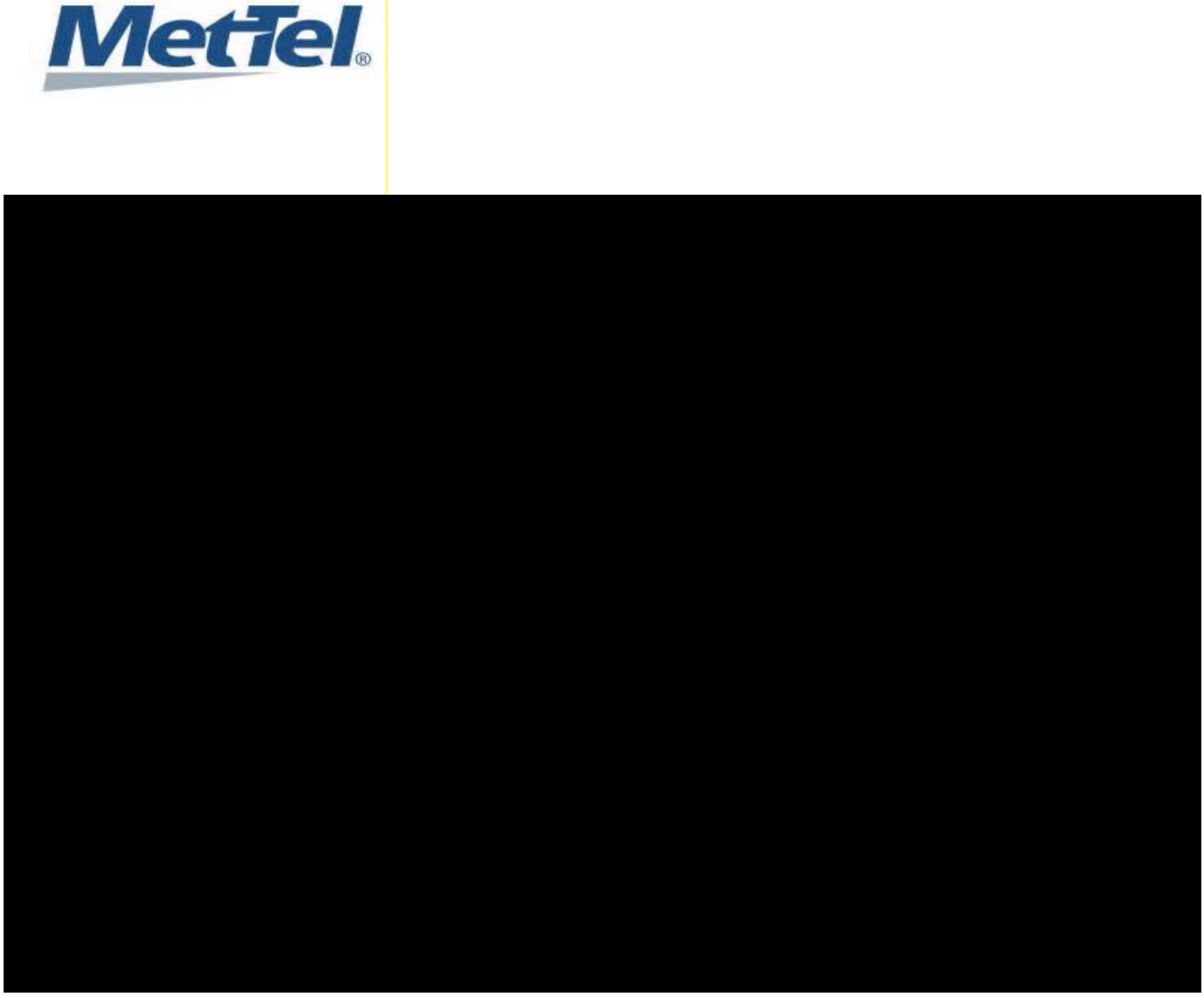
1. We agree that we may not publish and/or disclose in any manner, without the CO's written approval, the details of any safeguards designed and/or developed by MetTel under the EIS contract or otherwise provided to the Government, except for disclosure to a consumer agency for the purposes of A&A verification.

2. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the contractor, we will provide the Government logical and physical access to the our facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits will include, but are not limited to, the following methods:
    - Authenticated and unauthenticated operating system/network vulnerability scans,
    - Authenticated and unauthenticated web application vulnerability scans,
    - Authenticated and unauthenticated database application vulnerability scans, and
    - Internal and external penetration testing.
3. We agree that Government personnel, or agents acting on behalf of the Government, may perform automated scans using Government operated equipment, and Government specified tools. If we perform our own automated scans or audits, results from these scans may, at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. MetTel agrees that its scanning tools and their configurations require Government approval. MetTel will provide, in full, all scans we initiate, and their results, in full, to the Government.

A7.1.5.1 Personnel Security Suitability

We will perform personnel security/suitability in accordance with FAR Part 52.204-9. We have experience managing personnel security requirements for our current Federal customers, [redacted]. All MetTel personnel with access to Government information which is within the security A&A boundary will successfully complete a background investigation in accordance with Homeland Security Presidential Directive-12 (HSPD-12), OMB guidance M-05-24, M-11-11 and as specified in GSA CIO Order 2100.1I and GSA Directive 9732.1D Suitability and Personnel Security. The Government is responsible for the cost of such background investigations.

Exhibit A7-11. Systems Security Compliance Policy



[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]	