

Defense Security Service
Office of the Designated
Approving Authority



**DSS ELECTRONIC COMMUNICATIONS
PLAN TEMPLATE**

March 2010

**DEFENSE SECURITY SERVICE
ELECTRONIC COMMUNICATIONS PLAN TEMPLATE**

Date:

Company:

Address:

Cage Code:

ODAA Unique Identifier:

TABLE OF CONTENTS

1. INTRODUCTION	5
2. PURPOSE	6
3. ROLES/PERSONNEL SECURITY	6
4. DETAILED SYSTEM DESCRIPTION/TECHNICAL OVERVIEW	6
5. IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	6
5.1 USER IDENTIFICATION AND AUTHENTICATION	6
5.2 DEVICE IDENTIFICATION AND AUTHENTICATION	6
5.3 IDENTIFIER MANAGEMENT	7
5.4 AUTHENTICATOR MANAGEMENT	7
5.5 ACCESS CONTROL POLICY AND PROCEDURES	8
5.6 ACCOUNT MANAGEMENT	8
5.7 ACCESS ENFORCEMENT	9
5.8 INFORMATION FLOW ENFORCEMENT	9
5.9 SEPARATION OF DUTIES	10
5.10 LEAST PRIVILEGE	10
5.11 UNSUCCESSFUL LOGIN ATTEMPTS	11
5.12 SYSTEM USE NOTIFICATION	11
5.13 SESSION LOCK	12
5.15 SUPERVISION AND REVIEW — ACCESS CONTROL	12
5.16 REMOTE ACCESS	12
5.17 USE OF EXTERNAL INFORMATION SYSTEMS	13
6. SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	14
6.1 SECURITY TRAINING	14
7. AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	15
7.1 AUDITABLE EVENTS	15
7.2 CONTENT OF AUDIT RECORDS	15
7.3 AUDIT STORAGE CAPACITY	15
7.4 AUDIT MONITORING, ANALYSIS, AND REPORTING	16
7.5 TIME STAMPS	16
7.6 PROTECTION OF AUDIT INFORMATION	16
7.7 CONTINUOUS MONITORING	16
8. CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	16
8.1 MONITORING CONFIGURATION CHANGES	17
8.2 ACCESS RESTRICTIONS FOR CHANGE	17
8.3 LEAST FUNCTIONALITY	17
9. INCIDENT RESPONSE	18
9.1 INCIDENT RESPONSE POLICY AND PROCEDURES	18
9.2 INCIDENT RESPONSE TRAINING	18
9.3 INCIDENT RESPONSE TESTING AND EXERCISES	18
9.4 INCIDENT HANDLING	18
9.5 INCIDENT MONITORING	19
9.6 INCIDENT REPORTING	19
9.7 INCIDENT RESPONSE ASSISTANCE	19
10. PHYSICAL AND ENVIRONMENTAL PROTECTION	19
10.1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	19

10.2 PHYSICAL ACCESS AUTHORIZATIONS	19
10.3 PHYSICAL ACCESS CONTROL	20
10.4 MONITORING PHYSICAL ACCESS.....	20
11. CONTINGENCY PLANNING AND OPERATION	20
11.1 CONTINGENCY PLANNING POLICY AND PROCEDURES	20
11.2 CONTINGENCY PLAN	20
11.3 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION.....	21
12. SYSTEM AND COMMUNICATIONS PROTECTIONS	21
12.1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	21
13. APPLICATION PARTITIONING (IF APPLICABLE)	21
13.1 INFORMATION REMNANCE	21
13.2 DENIAL OF SERVICE PROTECTION.....	22
13.3 BOUNDARY PROTECTION	22
13.4 TRANSMISSION INTEGRITY	23
13.5 TRANSMISSION CONFIDENTIALITY	23
13.6 NETWORK DISCONNECT	23
13.7 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	23
13.8 COLLABORATIVE COMPUTING.....	24
13.9 MOBILE CODE	24
13.10 VOICE OVER INTERNET PROTOCOL.....	24
13.11 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE	24
13.12 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE.....	24
13.13 SESSION AUTHENTICITY	25
13.14 MALICIOUS CODE PROTECTION	25
13.15 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES	26
14. MAINTENANCE.....	27
14.1 SYSTEM MAINTENANCE POLICY AND PROCEDURES.....	27
14.2 CONTROLLED MAINTENANCE.....	27
14.3 MAINTENANCE TOOLS.....	28
14.4 REMOTE MAINTENANCE	28
14.5 MAINTENANCE PERSONNEL	29
15. MEDIA PROTECTION.....	29
15.1 MEDIA PROTECTION POLICY AND PROCEDURES.....	29
15.2 MEDIA ACCESS	29
15.3 MEDIA SANITIZATION AND DISPOSAL.....	30
16. EXPORT CONTROL PROCEDURES	30
17. ADDITIONAL FOCI PROCEDURES	30
17.1 TELEPHONE PROCEDURES.....	30
17.2 FACSIMILE PROCEDURES	30
17.3 COMPUTER COMMUNICATIONS	31
ATTACHMENT 1 – NETWORK DIAGRAM	32
ATTACHMENT 2 – EXPORT RELEASE FORMS.....	33
ATTACHMENT 3 – USER ACKNOWLEDGEMENT	34

1. INTRODUCTION

We have agreed with the Defense Security Service (DSS) to adopt this Electronic Communications Plan (ECP) in connection with our [*Describe applicable FOCI mitigation agreement*]. *The ECP template applies only to unclassified systems and can be modified to meet the facilities needs. Items that do not apply may be annotated as “Not Applicable.”*

Set forth herein are written policies and procedures that provide assurance to the Government Security Committee (GSC) and DSS that electronic communications between us or our subsidiaries and our parents or their affiliates (i) do not result in unauthorized disclosure of classified information or export controlled information, (ii) do not otherwise violate any OPSEC requirement; and (iii) are not used by our parents and/or their affiliates to exert influence or control over our business or management in a manner that could adversely affect the performance of classified contracts. This ECP includes a detailed network description and configuration diagram that clearly delineates which networks will be shared and which will be protected from foreign access. The network description contained herein addresses firewalls, remote administration, monitoring, maintenance, and separate e-mail servers, as appropriate. The scope of this ECP includes communications by telephone, teleconference, video conferences, facsimile, cell phones, PDAs and all computer communication including emails and server access. Teleconferences and video conferences must also be logged as visits under the visitation requirements of our FOCI mitigation agreement.

Our ECP adopts a systems approach based on the template published by DSS to assist us with describing our electronic communications at the appropriate level of detail to allow adequate assurances that we are in compliance with the terms of our mitigation agreement. The set of issues addressed herein is derived from that National Institute of Standards and Technology Publication: 800-53 (Appendix 2).

The ECP must reflect the following:

- *The ECP must describe in writing policies and procedures in place to ensure that company communications comply with the terms of the FOCI mitigation agreement.*
- *The requirements for the ECP differ based on the FOCI mitigation agreement.*
- *Under an SSA, sharing services between the foreign parent and cleared entities can be granted by DSS if the policies and procedures of the company can ensure that electronic communications will not be used by the Parent company or any of its affiliates to influence or control classified work and export controlled information.*
- *Under a PA, sharing of services between the foreign parent and cleared entities is not permitted in order to ensure that the Proxy Holders can exercise all prerogatives of management with complete independence from any foreign influence and control.*

- *All ECPs must cover communications by telephone, teleconference, video conference, facsimile and computer communication including emails and server access. Teleconference and video conferences must also be logged as visits under the visitation requirements of a mitigation agreement.*

2. PURPOSE

Instructions: In place of these instructions, please describe the Company's specific requirements from the mitigation agreement, the electronic communications of the company, and how the company intends to comply with the terms of the mitigation agreement. Identify the persons and entities whose electronic communications are subject to the ECP requirements of the Company's mitigation agreement.

3. ROLES/PERSONNEL SECURITY

Instructions: In place of these instructions, please describe specific points of contact with phone numbers and email addresses identifying the FSO, TCO, IT Personnel, and Outside Directors etc.

4. DETAILED SYSTEM DESCRIPTION/TECHNICAL OVERVIEW

Instructions: In place of these instructions, please describe all resources and servers that will be shared identifying all associated facilities, locations and legal entities.

5. IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES

Instructions: In place of these instructions, please describe how the Company will develop, disseminate, and periodically review and update: (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organization entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.

5.1 USER IDENTIFICATION AND AUTHENTICATION

To Company: In place of this instructional statement, please describe how the Company's information system will uniquely identify and authenticate users (or process acting on behalf of users).

5.2 DEVICE IDENTIFICATION AND AUTHENTICATION

Instructions: In place of these instructions, please describe how the Company's information system will identify and authenticate specific devices before establishing a connection. You may describe, for example, how the Company's information system will use either shared known

information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an Organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks.

5.3 IDENTIFIER MANAGEMENT

Instructions: In place of these instructions, please describe how the Company will manage user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate Contractor official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after [state time period] of inactivity; and (vi) archiving user identifiers.

5.4 AUTHENTICATOR MANAGEMENT

Instructions: In place of these instructions, please describe how the Company will manage information system authenticators by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically. You may describe for example, the following:

- *How the Company's information system authenticators include, tokens, PKI certificates, biometrics, passwords, and key cards.*
- *How users take reasonable measures to safeguard authenticators including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately.*
- *For password-based authentication, how the company's information system: (i) protects passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibits passwords from being displayed when entered; (iii) enforces password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations.*
- *For PKI-based authentication, the Company's information system: (i) validates certificates by constructing a certification path to an accepted trust anchor; (ii) establishes user control of the corresponding private key; and (iii) maps the authenticated identity to the user account.*
- *How authentication of public users accessing our information systems (and associated authenticator management) is required to protect nonpublic or privacy-related information.*

5.5 ACCESS CONTROL POLICY AND PROCEDURES

Instructions: In place of these instructions, please describe how the Company will develop, disseminate, and periodically review and update: (i) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

5.6 ACCOUNT MANAGEMENT

Instructions: In place of these instructions, please describe how the Company will manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. We will review information system accounts [state frequency, at least annually]. You may describe, for example, the following:

- *How the Company's account management will include the identification of account types (i.e., individual, group, and system), establishment of conditions for group membership, and assignment of associated authorizations.*
- *How the Company will identify authorized users of the information system and specifies access rights/privileges.*
- *How the Company will grant access to its information system based on: (i) a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria; and (ii) intended system usage.*
- *How the Company will require proper identification for requests to establish information system accounts and approves all such requests.*
- *How the Company will specifically authorize and monitor the use of guest/anonymous accounts and removes, disables, or otherwise secures unnecessary accounts.*
- *How the Company's account managers will be notified when information system users are terminated or transferred and associated accounts are removed, disabled, or otherwise secured.*
- *How the Company's account managers will be notified when users' information system usage or need-to-know/need-to-share changes."*

You may also explain how the Company will use the following control elements to manage accounts:

- (1) *Automated mechanisms to support the management of information system accounts.*

(2) An information system that will automatically terminate temporary and emergency accounts after [state time period for each type of account].

(3) An information system that will automatically disable inactive accounts after [state time period].

(4) Automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals.

5.7 ACCESS ENFORCEMENT

Instructions: In place of these instructions, please describe how the Company's information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy. You may describe, for example, the following:

- How access control policies (e.g., identity-based policies, role-based policies, rule-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) are employed by the Company to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system.*
- How, in addition to controlling access at the information system level, access enforcement mechanisms are employed at the application level, when necessary, to provide increased information security for the Company.*

You may also explain how the Company will use the following control element to manage access enforcement:

- An information system that restricts access to privileged functions (deployed in hardware, software, and firmware) and security-relevant information to explicitly authorized personnel, including, for example, security administrators, system and network administrators, and other privileged users. Privileged users are individuals who have access to system control, monitoring, or administration functions (e.g., system administrators, information system security officers, maintainers, system programmers). [Company should also list each responsible individual by name.]*

5.8 INFORMATION FLOW ENFORCEMENT

Instructions: In place of these instructions, please describe how the Company's information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. You may describe, for example, the following:

- How the Company's information flow will control where information is allowed to travel within an information system and between information systems (as opposed to who is*

allowed to access the information) and without explicit regard to subsequent accesses to that information.

- *How the Company will keep export controlled information from being transmitted in the clear to the Internet, block outside traffic that claims to be from within the Company, and not pass any web requests to the Internet that are not from the internal web proxy.*
- *How the Company's information flow control policies and enforcement mechanisms will control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems.*
- *How the Company's flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services or provide a packet filtering capability.*

5.9 SEPARATION OF DUTIES

Instructions: In place of these instructions, please describe how the Company's information system enforces separation of duties through assigned access authorizations. You may describe, for example, the following:

- *How the Company will establish appropriate divisions of responsibility and separate duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.*
- *How there is access control software on the Company's information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion.*
- *How the Company will divide mission functions and distinct information system support functions among different individuals/roles.*
- *How the Company will have different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security)*
- *How the Company will use security personnel to administer access control functions who are different from the personnel who administer the Company's audit functions.*

5.10 LEAST PRIVILEGE

Instructions: In place of these instructions, please describe how the Company's information system will enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks. You may describe,

for example, how the Company employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals.

5.11 UNSUCCESSFUL LOGIN ATTEMPTS

Instructions: In place of these instructions, please describe how the Company's information system will enforce a limit of [state the appropriate number] consecutive invalid access attempts by a user during a [state the appropriate time period] time period. You may describe, for example, the following:

- *How the Company's information system (i) will automatically lock the account/node for an [state the appropriate time period] and/or delay next login prompt according to [state the appropriate delay algorithm] when the maximum number of unsuccessful attempts is exceeded.*
- *Whether automatic lockouts initiated by the information system will be temporary and automatically release after a predetermined time period established by the Company.*

5.12 SYSTEM USE NOTIFICATION

Instructions: In place of these instructions, please describe how the Company's information system will display an approved, system use notification message before granting system access informing potential users of the following: (i) that the user is accessing information system; (ii) that system usage may be monitored, recorded, and subject to audit; (iii) that unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) that use of the system indicates consent to monitoring and recording.

You may describe, for example, the following:

- *How the Company's privacy and security policies will be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.*
- *How the Company's system use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system.*
- *How the Company's system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and will remain on the screen until the user takes explicit actions to log on to the information system.*
- *For the Company's publicly accessible systems: (i) how the system use information will be available and when appropriate, will be displayed before granting access; (ii) how any references to monitoring, recording, or auditing will be in keeping with privacy accommodations for such systems that generally prohibit those activities; and (iii) how*

the notice given to public users of the information system will include a description of the authorized uses of the system.

5.13 SESSION LOCK

Instructions: In place of these instructions, please describe how the Company's information system will prevent further access to the system by initiating a session lock after [state appropriate time period] of inactivity, and the session lock will remain in effect until the user reestablishes access using appropriate identification and authentication procedures.

You may describe, for example, how the Company's users will be able to directly initiate session lock mechanisms. It is recommended that Company not consider a session lock as a substitute for logging out of the information system. Moreover, Company policy in this respect should, where possible, be consistent with federal policy; for example, in accordance with OMB Memorandum 06-16, the time period of inactivity resulting in session lock is no greater than thirty minutes for remote access and portable devices.

5.14 SESSION TERMINATION

Instructions: In place of these instructions, please describe how the Company's information system will automatically terminate a remote session after [state appropriate time period] of inactivity. Company should consider a remote session to have been initiated whenever an organizational information system is accessed by a user (or an information system) communicating through an external, network not under the control of the Company such as the Internet.

5.15 SUPERVISION AND REVIEW — ACCESS CONTROL

Instructions: In place of these instructions, please describe how the Company will supervise and review the activities of users with respect to the enforcement and usage of information system access controls. You may describe, for example, the following:

- *How the Company will review audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures.*
- *How the Company will investigate any unusual information system-related activities and periodically reviews changes to access authorizations.*
- *How the Company will employ automated mechanisms to facilitate the review of user activities.*

5.16 REMOTE ACCESS

Instructions: In place of these instructions, please describe how the Company will authorize, monitor, and control all methods of remote access to the information system. The Company should consider remote access to include any access to an organizational information system by

a user (or an information system) communicating through an external, network not under the control of the Company such as the Internet. Examples of remote access methods include dial-up, broadband, and wireless. Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access.

You may describe, for example, the following:

- *How the Company will restrict access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections (e.g., using virtual private network technology).*
- *How the Company will employ automated mechanisms to facilitate the monitoring and control of remote access methods.*
- *How the Company will use cryptography to protect the confidentiality and integrity of remote access sessions.*
- *How the Company will control all remote accesses through a limited number of managed access control points.*
- *How the Company will permit remote access for privileged functions only for compelling operational needs and documents the rationale for such access in the security plan for the information system.*

5.17 USE OF EXTERNAL INFORMATION SYSTEMS

Instructions: In place of these instructions, please describe how the Company will establish terms and conditions for authorized individuals to: (i) access the information system from an external information system; and (ii) process, store, and/or transmit Company-controlled information using an external information system.

You may describe, for example, the following:

- *Whether any of the Company's external information systems will be information systems or components of information systems for which the Company has no direct control over the application of required security controls or the assessment of security control effectiveness.*
- *Whether any of the Company's external information systems will include, without limitation, personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); information systems owned or controlled by nonfederal governmental contractors; and federal information systems that are not owned by, operated by, or under the direct control of the Company.*

- *Whether any of the Company's authorized individuals will include Contractor personnel, contractors, or any other individuals with authorized access to the Contractor's information system and information that is not intended for public access.*
- *Whether the Company will establish terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The Company should establish terms and conditions that will address as a minimum the types of applications that can be accessed on the organizational information system from the external information system.*

You may also explain how the Company will use the following control element to manage use of external information systems:

- *A prohibition on authorized individuals using an external information system to access the information system or to process, store, or transmit Company-controlled information except in situations where the Company: (i) can verify the employment of required security controls on the external system as specified in the Company's information security policy and system security plan; or (ii) has approved information system connection or processing agreements with the Company entity hosting the external information system.*

6. SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Instructions: In place of these instructions, please describe how the Company will develop, disseminate, and periodically review/update: (i) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Contractor entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls. You may describe, for example, how the Company's security awareness and training policy and procedures will be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

6.1 SECURITY TRAINING

Instructions: In place of these instructions, please describe how the Company will identify personnel that have significant information system security roles and responsibilities during the system development life cycle, document those roles and responsibilities, and provide appropriate information system security training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) [state appropriate frequency] thereafter. You may describe, for example, the following:

- *How the Company will determine the appropriate content of security training based on its specific requirements and the information systems to which personnel have authorized access.*

- *How the Company will provide system managers, system and network administrators, and other personnel having access to system-level software, adequate technical training to perform their assigned duties.*
- *How the Company will require a signed acknowledgement by personnel receiving security awareness training.*

7. AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES

Instructions: In place of these instructions, please describe how the Company will develop, disseminate, and periodically review/update: (i) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Contractor entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls. You may describe, for example, how the Company's audit and accountability policy and procedures will be consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

7.1 AUDITABLE EVENTS

Instructions: In place of these instructions, please describe how the Company's information system will generate audit records for the following events: [list applicable events]. You may describe, for example, how the Company will (i) define auditable events that are adequate to support after-the-fact investigations of security incidents and (ii) periodically review and update the list of defined auditable events.

7.2 CONTENT OF AUDIT RECORDS

Instructions: In place of these instructions, please describe how the Company's information system will produce audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events. You may describe, for example, how the Company's audit record content will include: (i) date and time of the event; (ii) the component of the information system (e.g., software component, hardware component) where the event occurred; (iii) type of event; (iv) user/subject identity; and (v) the outcome (success or failure) of the event.

7.3 AUDIT STORAGE CAPACITY

Instructions: In place of these instructions, please describe how the Company will allocate sufficient audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded. You may describe, for example, how the Company will provide sufficient audit storage capacity, taking into account the auditing to be performed and the online audit processing requirements.

7.4 AUDIT MONITORING, ANALYSIS, AND REPORTING

Instructions: In place of these instructions, please describe how the Company will regularly review/analyze information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions. You may describe, for example, how the Company will employ automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [Provide a list inappropriate or unusual activities that are to result in alerts].

7.5 TIME STAMPS

Instructions: In place of these instructions, please describe how the Company's information system will provide time stamps for use in audit record generation. You may describe, for example, the following:

- *How the Company's time stamps (including date and time) of audit records will be generated using internal system clocks.*
- *How the Company will synchronize its internal information system clocks every: [state appropriate frequency].*

7.6 PROTECTION OF AUDIT INFORMATION

Instructions: In place of these instructions, please describe how the Company's information system will protect audit information and audit tools from unauthorized access, modification, and deletion. You may describe, for example, how the Company's audit information will include all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity.

7.7 CONTINUOUS MONITORING

Instructions: In place of these instructions, please describe how the Company will monitor the security controls in the information system on an ongoing basis. You may describe, for example, the following:

- *How the Company will use continuous monitoring activities such as: configuration management and control of information system components, security impact analyses of changes to the system, ongoing assessment of security controls, and status reporting.*
- *How the Contractor will assess all security controls in an information system.*

8. CONFIGURATION MANAGEMENT POLICY AND PROCEDURES

Instructions: In place of these instructions, please describe how the Company will develop, disseminate, and periodically review/update: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Contractor entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

8.1 MONITORING CONFIGURATION CHANGES

Instructions: In place of these instructions, please describe how the Company's [Contractor Name] monitors changes to the information system conducting security impact analyses to determine the effects of the changes. You may describe, for example, the following:

- *How, prior to change implementation, and as part of the change approval process, the Company will analyze changes to the information system for potential security impacts.*
- *How, after the information system is changed (including upgrades and modifications), the Company will check the security features to verify that the features are still functioning properly.*
- *How the Company will audit activities associated with configuration changes to the information system. Monitoring configuration changes and conducting security impact analyses are important elements with regard to the ongoing assessment of security controls in the information system.*

8.2 ACCESS RESTRICTIONS FOR CHANGE

Instructions: In place of these instructions, please describe how the Company will: (i) approve individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generate, retain, and review records reflecting all such changes. You may describe, for example, the following:

- *How planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system.*
- *How only qualified and authorized individuals will be able to obtain access to information system components for purposes of initiating changes, including upgrades, and modifications.*

8.3 LEAST FUNCTIONALITY

Instructions: In place of these instructions, please describe how the Company will configure the information system to provide only essential capabilities and specifically prohibits and/or restrict the use of the following functions, ports, protocols, and/or services: [Provide applicable list of prohibited and/or restricted functions, ports, protocols, and/or services].

9. INCIDENT RESPONSE

9.1 INCIDENT RESPONSE POLICY AND PROCEDURES

Instructions: In place of these instructions, please describe how the Company will develop, disseminate, and periodically review/update: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Company entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls. You may describe, for example, how the Company's incident response policy and procedures will be consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.

Note: The Contractor's incident response policy can be included as part of its general information security policy. Incident response procedures can be developed for the security program in general, and for a particular information system, when required.

9.2 INCIDENT RESPONSE TRAINING

Instructions: In place of these instructions, please describe how the Company will train personnel in their incident response roles and responsibilities with respect to the information system and provide refresher training [Provide appropriate frequency, at least annually].

9.3 INCIDENT RESPONSE TESTING AND EXERCISES

Instructions: In place of these instructions, please describe how the Company will test and/or exercise the incident response capability for the information system [Provide appropriate frequency, at least annually] using [Provide appropriate description] tests to determine the incident response effectiveness and documents the results. You may describe, for example, whether the Company will use NIST Special Publication 800-84 as supplemental guidance on its test, training, and exercise programs for information technology plans and capabilities.

9.4 INCIDENT HANDLING

Instructions: In place of these instructions, please describe how the Company will implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. You may describe, for example, the following:

- *How the Company will incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.*
- *How the Contractor will employ automated mechanisms to support the incident handling process.*

Note: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

9.5 INCIDENT MONITORING

Instructions: In place of these instructions, please describe how the Company will track and document information system security incidents on an ongoing basis.

9.6 INCIDENT REPORTING

Instructions: In place of these instructions, please describe how the Company will promptly report incident information to appropriate authorities. You may describe, for example, how the Company will use automated mechanisms to assist in the reporting of security incidents.

9.7 INCIDENT RESPONSE ASSISTANCE

Instructions: In place of these instructions, please describe how the Company will provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. (The support resource is an integral part of the Company's incident response capability.) You may describe, for example, how the Company will support incident response through (i) a help desk or an assistance group and (ii) access to forensics services as needed.

10. PHYSICAL AND ENVIRONMENTAL PROTECTION

10.1 PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES

Instructions: In place of these instructions, please describe how the Company will develop, disseminate, and periodically review/update: (i) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Company entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

10.2 PHYSICAL ACCESS AUTHORIZATIONS

Instructions: In place of these instructions, please describe how the Company will develop and keep current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issues appropriate authorization credentials. You may describe, for example, the following:

- *How the Company will define the appropriate authorization credentials (for example, badges, identification cards, and smart cards).*

- *How Company will promptly remove from the access list personnel no longer requiring access to the facility where the information system resides.*
- *How designated officials within the Company will review and approve the access list and authorization credentials [state appropriate frequency, at least annually].*

10.3 PHYSICAL ACCESS CONTROL

Instructions: In place of these instructions, please describe how the Company will control all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verify individual access authorizations before granting access to the facility. You may describe, for example, how the Company will control access to areas officially designated as publicly accessible, as appropriate, in accordance with the Company's assessment of risk.

10.4 MONITORING PHYSICAL ACCESS

Instructions: In place of these instructions, please describe how the Company will monitor physical access to the information system to detect and respond to physical security incidents. You may describe, for example, the following:

- *How the Company will review physical access logs periodically and investigate apparent security violations or suspicious physical access activities.*
- *How response to detected physical security incidents will be a part of the Company's incident response capability.*
- *How the Company will monitor real-time physical intrusion alarms and surveillance equipment.*

11. CONTINGENCY PLANNING AND OPERATION

11.1 CONTINGENCY PLANNING POLICY AND PROCEDURES

Instructions: In place of these instructions, please describe how the Company will develop, disseminate, and periodically review/update: (i) a formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Company entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. You may describe, for example, how the Company's contingency planning policy and procedures are consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.

11.2 CONTINGENCY PLAN

Instructions: In place of these instructions, please describe how the Company will develop and implement a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. You may describe, for example, how designated officials within the Company will review and approve the contingency plan and distribute copies of the plan to key contingency personnel.

11.3 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION

Instructions: In place of these instructions, please describe how the Company will employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure.

12. SYSTEM AND COMMUNICATIONS PROTECTIONS

12.1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES

Instructions: In place of these instructions, please describe how the Company will develop, disseminate, and periodically review/update: (i) a formal, documented, system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Company entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls. You may describe, for example, how the Company's system and communications protection policy and procedures will be consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.

13. APPLICATION PARTITIONING (IF APPLICABLE)

Instructions: In place of these instructions, please describe how the Company's information system will separate user functionality (including user interface services) from information system management functionality. You may describe, for example, how the Company's information system will physically or logically separate user interface services (e.g., public web pages) from information storage and management services (e.g., database management). Note: Separation may be accomplished through the use of different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

13.1 INFORMATION REMNANCE

Instructions: In place of these instructions, please describe how the Company's information system will prevent unauthorized and unintended information transfer via shared system resources. You may describe, for example, how the Company will control information system remnance, sometimes referred to as object reuse, or data remnance, in order to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being

available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system.

13.2 DENIAL OF SERVICE PROTECTION

Instructions: In place of these instructions, please describe how the Company's information system will protect against or limits the effects of the following types of denial of service attacks: [please list types of denial of service attacks or reference to source for current list]. You may also describe, for example, the following:

- *How the Company will use a variety of technologies to limit, or in some cases, eliminate the effects of denial of service attacks.*
- *How the Company will use boundary protection devices to filter certain types of packets to protect devices on the Company's internal network from being directly affected by denial of service attacks.*
- *How the Company's information systems that are publicly accessible will be protected by employing increased capacity and bandwidth combined with service redundancy.*

13.3 BOUNDARY PROTECTION

Instructions: In place of these instructions, please describe how the Company's information system will monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. You may describe, for example, the following:

- *How the Company will use connections to the Internet, or other external networks or information systems, that occur through managed interfaces consisting of appropriate boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels) arranged in an effective architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ).*
- *How the Company will use information system boundary protections at any designated alternate processing sites provide the same levels of protection as that of the primary site.*
- *How the Company will consider the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services.*
- *How the Company will use commercial telecommunications services that are commonly based on network components and consolidated management systems shared by all*

attached commercial customers, and may include third party provided access lines and other service elements.

You may also explain how the Company will use the following control elements to protect information system boundaries:

- (1) Physical allocation of publicly accessible information system components to separate subnetworks with separate, physical network interfaces.*
- (2) Prevention of public access into the Company's internal networks except as appropriately mediated.*
- (3) Limits on the number of access points to the information system to allow for better monitoring of inbound and outbound network traffic.*
- (4) A managed interface (boundary protection devices in an effective security-architecture) with any external telecommunication service, implementing controls appropriate to the required protection of the confidentiality and integrity of the information being transmitted.*
- (5) An information system that denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).*

13.4 TRANSMISSION INTEGRITY

Instructions: In place of these instructions, please describe how the Company's information system will protect the integrity of transmitted information.

13.5 TRANSMISSION CONFIDENTIALITY

Instructions: In place of these instructions, please describe how the Company's information system will protect the confidentiality of transmitted information.

13.6 NETWORK DISCONNECT

Instructions: In place of these instructions, please describe how the Company's information system will terminate a network connection at the end of a session or after [state appropriate time period] of inactivity. You may describe, for example, whether and how the Company will apply this control within the context of risk management that considers specific mission or operational requirements.

13.7 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

Instructions: In place of these instructions, please describe how the Company will establish and manage cryptographic keys (when cryptography is required and employed within the

information system) using automated mechanisms with supporting procedures or manual procedures.

13.8 COLLABORATIVE COMPUTING

Instructions: In place of these instructions, please describe, if applicable, how the Company's information system will prohibit remote activation of collaborative computing mechanisms and provides an explicit indication of use to the local users. You may describe, for example, how the Company's collaborative computing mechanisms, if any, will include, for example, video and audio conferencing capabilities. Note: explicit indication of use includes, for example, signals to local users when cameras and/or microphones are activated.

13.9 MOBILE CODE

Instructions: In place of these instructions, please describe how the Company will (i) establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorize, monitor, and control the use of mobile code within the information system.

13.10 VOICE OVER INTERNET PROTOCOL

Instructions: In place of these instructions, please describe how the Company will (i) establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) authorize, monitor, and control the use of VoIP within the information system.

13.11 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)

Instructions: In place of these instructions, please describe how the Company's information system will provide name/address resolution service and additional data origin and integrity artifacts along with the authoritative data it returns in response to resolution queries. You may describe, for example, how the Company will enable remote clients to obtain origin authentication and integrity verification assurances for the name/address resolution information obtained through the service. Note: A domain name system (DNS) server is an example of an information system that provides name/address resolution service; digital signatures and cryptographic keys are examples of additional artifacts; and DNS resource records are examples of authoritative data.

13.12 ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE

Instructions: In place of these instructions, please describe how the Company's information systems will collectively provide name/address resolution service for the Company that are fault tolerant and implement role separation. You may describe, for example, the following:

- *How the Company will use a domain name system (DNS) server as an information system that provides name/address resolution service.*
- *To eliminate single points of failure and to enhance redundancy, how the Company will use at least two authoritative domain name system (DNS) servers, one configured as primary and the other as secondary.*
- *How the Company will use two servers located in two different network subnets and geographically separated (i.e., not located in the same physical facility).*
- *If the Company's information technology resources are divided into those resources belonging to internal networks and those resources belonging to external networks, how the Company will use authoritative DNS servers with two roles (internal and external). Explain (i) how the Company's DNS server with the internal role will provide name/address resolution information pertaining to both internal and external information technology resources while the DNS server with the external role only provides name/address resolution information pertaining to external information technology resources and (ii) specify the list of clients who can access the authoritative DNS server of a particular role.*

13.13 SESSION AUTHENTICITY

Instructions: In place of these instructions, please describe how the Company's information system will provide mechanisms to protect the authenticity of communications sessions. You may describe, for example, how the Company will focus its session authenticity controls on communications protection at the session, versus packet, level in order to implement session-level protection where needed (e.g., in service-oriented architectures providing web-based services).

13.14 MALICIOUS CODE PROTECTION

Instructions: In place of these instructions, please describe how the Company's information system will implement malicious code protection. You may describe, for example, the following:

- *How the Company will employ malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network.*
- *How the Company will use the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB devices, diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities.*

- *How the Company will update malicious code protection mechanisms (including the latest virus definitions) whenever new releases are available in accordance with Company configuration management policy and procedures.*
- *How the Company will use malicious code protection software products from multiple vendors (e.g., using one vendor for boundary devices and servers and another vendor for workstations).*

13.15 INFORMATION SYSTEM MONITORING TOOLS AND TECHNIQUES

Instructions: In place of these instructions, please describe how the Company's [Contractor Name] employs tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system. You may describe, for example, the following:

- *How the Company's information system monitoring capability will be achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software).*
- *How the Company's monitoring devices will be strategically deployed within the information system (e.g., at selected perimeter locations, near server farms supporting critical applications) to collect essential information. How the Company's monitoring devices will be deployed at ad hoc locations within the system to track specific transactions.*
- *How the Company's monitoring devices will be used to track the impact of security changes to the information system.*
- *How the granularity of the information collected will be determined by the Company based upon its monitoring objectives and the capability of the information system to support such activities.*
- *How the Company will consult appropriate legal counsel with regard to all information system monitoring activities.*
- *How the Company will heighten the level of information system monitoring activity whenever there is an indication of increased risk to operations, assets, or individuals based on law enforcement information, intelligence information, or other credible sources of information.*
- *How the Company's information system will monitor inbound and outbound communications for unusual or unauthorized activities or conditions. Note: Unusual/unauthorized activities or conditions include, for example, the presence of malicious code, the unauthorized export of information, or signaling to an external information system.*

14. MAINTENANCE

14.1 SYSTEM MAINTENANCE POLICY AND PROCEDURES

Instructions: In place of these instructions, please describe how the Company will develop, disseminate, and periodically review/update: (i) a formal, documented, information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Company entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls. You may describe, for example, the following:

- *How the Company's information system maintenance policy and procedures will be consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.*
- *How the Company's information system maintenance policy will be included as part of its general information security policy.*
- *How the Company's system maintenance procedures will be developed for the security program in general, and for a particular information system, when required.*
- *How the Company will require maintenance personnel to be a U.S. citizen under direct contract with the Company or through entities organized and existing in the United States.*
- *How the Company will require each maintenance personnel to be a U.S. citizen and under contract with the Company directly or through entities organized and existing in the United States..*

14.2 CONTROLLED MAINTENANCE

Instructions: In place of these instructions, please describe how the Company will schedule, perform, document, and review records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or Company requirements. You may describe, for example, the following:

- *How the Company's maintenance activities, including without limitation routine, scheduled maintenance and repairs will be controlled.*
- *Whether the Company's maintenance activities will be performed on site or remotely and whether the equipment is serviced on site or removed to another location.*
- *How Company officials will approve the removal of the information system or information system components from the facility when repairs are necessary.*

- *If the information system or component of the system requires off-site repair, how the Company will remove all information from associated media using approved procedures. After maintenance is performed on the information system, how the Company will check all potentially impacted security controls to verify that the controls are still functioning properly.*
- *How the Company will maintain maintenance records for the information system that include: (i) the date and time of maintenance; (ii) name of the individual performing the maintenance; (iii) name of escort, if necessary; (iv) a description of the maintenance performed; and (v) a list of equipment removed or replaced (including identification numbers, if applicable).*

14.3 MAINTENANCE TOOLS

Instructions: In place of these instructions, please describe how the Company will approve, control, and monitor the use of information system maintenance tools and maintains the tools on an ongoing basis. You may describe, for example, how the Company will address hardware and software brought into the information system specifically for diagnostic/repair actions (e.g., a hardware or software packet sniffer that is introduced for the purpose of a particular maintenance activity). Note: Hardware and/or software components that may support information system maintenance, yet are a part of the system (e.g., the software implementing “ping,” “ls,” “ipconfig,” or the hardware and software implementing the monitoring port of an Ethernet switch) are not covered by this control.

14.4 REMOTE MAINTENANCE

Instructions: In place of these instructions, please describe how the Company will authorize, monitor, and control any remotely executed maintenance and diagnostic activities, if employed. You may describe, for example, the following:

- *How the Company’s remote maintenance and diagnostic activities will be conducted by individuals communicating through an external, non-Company-controlled network (e.g., the Internet).*
- *How the Company’s remote maintenance and diagnostic tools will be used, and its use documented, consistent with its organizational policy.*
- *How the Company will maintain records for all remote maintenance and diagnostic activities.*
- *How the Company will use other techniques and/or controls for improving the security of remote maintenance including without limitation: (i) encryption and decryption of communications; (ii) strong identification and authentication techniques (such as Level 3 or 4 tokens as described in NIST Special Publication 800-63); and (iii) remote disconnect verification.*

- *When remote maintenance is completed, how the Company (or its system) will terminate all sessions and remote connections invoked in the performance of that activity.*
- *How the Company will audit all remote maintenance and diagnostic sessions and appropriate Contractor personnel review the maintenance records of the remote sessions.*
- *How the Company will address the installation and use of remote maintenance and diagnostic links.*

14.5 MAINTENANCE PERSONNEL

Instructions: In place of these instructions, please describe how the Company will allow only authorized personnel to perform maintenance on the information system. You may describe, for example, the following:

- *How the Company's maintenance personnel (whether performing maintenance locally or remotely) will receive appropriate access authorizations to the information system when maintenance activities allow access to Company information or could result in a future compromise of confidentiality, integrity, or availability.*
- *When maintenance personnel do not have needed access authorizations, how Contractor personnel with appropriate access authorizations will supervise maintenance personnel during the performance of maintenance activities on the information system.*

15. MEDIA PROTECTION

15.1 MEDIA PROTECTION POLICY AND PROCEDURES

Instructions: In place of these instructions, please describe how the Company will develop, disseminate, and periodically review/update: (i) a formal, documented, media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among Company entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls. You may describe, for example, how the Company's media protection policy and procedures will be consistent with applicable federal laws, directives, policies, regulations, standards, and guidance.

15.2 MEDIA ACCESS

Instructions: In place of these instructions, please describe how the Company will (i) restrict access to information system media to authorized individuals and (ii) employ automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

15.3 MEDIA SANITIZATION AND DISPOSAL

Instructions: In place of these instructions, please describe how the Company will sanitize information system media, both digital and non-digital, prior to disposal or release for reuse. You may describe, for example, the following:

- *How the Company's sanitization process will remove information from information system media so there is reasonable assurance, in proportion to the confidentiality of the information, that the information cannot be retrieved or reconstructed.*
- *How the Company's sanitization techniques, including clearing, purging, and destroying media information, will prevent the disclosure of Company information to unauthorized individuals when such media is reused or disposed.*

16. EXPORT CONTROL PROCEDURES

Instructions: In place of these instructions, please describe or reference the document containing the Company's export control procedures as applicable.

17. ADDITIONAL FOCI PROCEDURES

17.1 TELEPHONE PROCEDURES

Instructions: In place of these instructions, please describe how the Company's maintains a log to reflect telephone activity between it or its subsidiaries, on the one hand, and its parent or affiliates of the parent on the other hand, in accordance with the specific requirements of the applicable FOCI mitigation agreement. You may describe, for example, the following:

- *How the log will be reviewed by the FSO, the GSC and DSS.*
- *How the log will include the Name, Position/Title of the Individual maintaining the log, the Name, Position/Title of the individual parties to the call, and brief remarks that reflect the general topic of the conversation.*
- *How a summary of this data will be prepared in support of the annual meeting report. Teleconferences and video teleconferences must be described here and logged under visits for the purposes of the mitigation agreement.*

17.2 FACSIMILE PROCEDURES

Instructions: In place of these instructions, please describe how the Company will maintain a log to reflect telephone activity between it or its subsidiaries, on the one hand, and its parent or affiliates of the parent on the other hand, in accordance with the specific requirements of the applicable FOCI mitigation agreement. You may describe, for example, the following:

- *How the log will be reviewed by the FSO, the GSC and DSS.*

- *How the log will include the Name, Position/Title of the Individual maintaining the log, the Name, Position/Title of the individual parties to the fax, and brief remarks that reflect the general topic of the fax.*
- *How a summary of this data will be prepared in support of the annual meeting report.*

17.3 COMPUTER COMMUNICATIONS

Instructions: In place of these instructions, please describe whether the Company will use Microsoft Outlook email, computer fax, VTC, instant messaging, FTP, and/or other applicable computer communication tools. You may describe, for example, the following:

- *How the Company's computer communication systems will be monitored and controlled to ensure compliance with the mitigation agreement.*
- *How the Company's computer network server for unclassified email of the cleared company will be owned by the cleared company and monitored using [describe monitoring software].*
- *How the Company's firewalls will be used to protect [describe specific access protected by firewalls].*

ATTACHMENT 1 – NETWORK DIAGRAM

ATTACHMENT 2 – EXPORT RELEASE FORMS

ATTACHMENT 3 – USER ACKNOWLEDGEMENT

**Special Security Agreement/Proxy Agreement Electronic Communications Plan
Acknowledgment**

I, _____, hereby acknowledge that I have read the Electronic Communications Plan. I understand that it is my responsibility to abide by the policies and requirements set forth in the Electronic Communications Plan. I am aware that I can seek additional guidance from the Facility Security Officer.

Signature

Date