March 2012

SECURITY CONTROL OVERLAYS TEMPLATE

Version 1

THIS DOCUMENT PRESCRIBES MINIMUM STANDARDS
YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER IMPLEMENTATION

FOREWORD

An overlay is a specification of security controls and supporting guidance used to complement the security control baselines and parameter values in Committee on National Security Systems Instruction (CNSSI) No. 1253 and to complement the supplemental guidance in National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-53. An overlay's specifications may be more stringent or less stringent than the controls and guidance complemented. Overlays may be applied to reflect the needs of different information types (e.g., personally identifiable information [PII], financial, or highly sensitive types of intelligence); system functionality needs (e.g., stand-alone systems, cross domain solutions, or controlled interface systems); or environmental or operationally-driven needs (e.g., tactical, space-based, or test environment).

This template is provided to assist in the development of overlays, to help ensure all of the required information is provided, and to support a consistent format for the overlays.

FOR THE NATIONAL MANAGER

//s//

DEBORA A. PLUNKETT

CNSS Secretariat (IE32). National Security Agency. 9800 Savage Road, STE 6716. Ft. Meade, MD 20755-6716
Office: (410) 854-6805 Unclassified FAX: (410) 854-6814
CNSS@radium.ncsc.mil

<Insert Name> Overlay

1. Characteristics and Assumptions

<Insert a paragraph that includes characteristics of the required use of the overlay. The level of detail in the description should be sufficient to justify the control selections.>

Guidance (delete when description is completed): Identify the characteristics that describe the required use of the overlay. This may include a description of the environment in which the overlay will be used (e.g., inside a guarded building within the continental United States, in a mobile vehicle in close proximity to adversaries, while traveling for business to a foreign country that is known for attempting to gain access to sensitive or classified information). The characteristics may also include a description of the type of information that will be processed within an information system (e.g., a system that contains personally identifiable information (PII), sensitive financial information, or health records). Another possible characteristic of overlays focuses on the functionality within the system (e.g., the system is a stand-alone system, type of platform IT, or a cross domain system).

An overlay may also be required to protect organizations, information, information systems, or individuals from different threats and vulnerabilities than typical information systems. The typical information system is adequately protected by the existing baselines. If an overlay is designed to address different threats and vulnerabilities, they should be identified and documented in this section of the overlay.

The level of detail in the description should be sufficient to justify the control selections. For example, an overlay based on the environment in which the system will operate should include details about the type and quality of connectivity, type of interface used within the system, storage capacity, characteristics of the physical environment such as the power source and availability of other utilities, types of hazards in the environment, inventory of spare parts, type and amount of training individuals will have, and a description of any additional operating requirements.

Sample (delete when description is completed):

Tactical overlays apply to systems that are being created for use in or that will be deployed to tactical environments. Examples of tactical environments include, but are not limited to, mobile command centers such as command and control aircraft and large deck ships, mobile platforms such as tanks and fighter jets, and dismounted environments such as platoons and soldiers on foot in war zones. Some of the distinguishing characteristics of tactical environments include significant size, weight, and power constraints, network bandwidth and connectivity constraints, processing and storage limitations, high operational tempo, harsh environmental conditions, frequent personnel turnover, data with high refresh rates and low persistent value, and the close physical proximity to the adversaries and the associated non-cyber threats.

While many controls from the baselines continue to apply in the tactical environments, how they are

implemented varies. Implementation varies because of differences in risk and in both technical and operational constraints. For example, because ships have little bandwidth it is not practical to automatically push all necessary security updates over the network. Instead, helicopters deliver CDs with the updates to the ship when necessary. Similarly, automatic updates in a tactical environment could be dangerous if the updates resulted in a system not working or interrupted on-going mission activities thereby compromising the success of the mission and the safety of the troops. In this case, updates should be delayed until after active operational missions have been completed. Other IA controls such as auditing must be carefully tailored to be sensitive to the limited storage and processing capacity of some tactical systems – resources that must be shared with critical mission functionality.

2. Applicability

<Insert text.>

Guidance (delete when the guidance is completed): Include a series of questions that can be used to determine whether or not the overlay applies to a system. The questions and possible answers should be supported by the overlay characteristics and assumptions. The questions and answers should lead to decision on whether or not the overlay applies to a specific system.

Sample (delete when description is completed):

The following questions are used to determine whether or not this overlay applies to your system:

1. Will the system be deployed to a tactical environment (e.g., war zone, peacekeeping activity, disaster relief, humanitarian aid)?
2. Will the size and weight of the system have to be limited due to constraints of the operational environment (e.g., it must fit within a small area on a command and control aircraft, must be carried by a soldier)?
3. Will the power supply be limited because it will not be possible to connect to a power grid (e.g., it will rely on a generator or batteries)?
4. Will the network connectivity be limited and the bandwidth low due to constraints of the operational environment?
5. Will the network connectivity be intermittent or unreliable?
6. Will the operational tempo be high (e.g., require 24-7 use of systems)?
7. Will the system be required to operate in extreme environmental conditions (e.g., heat, salt, humidity, altitude, vibration)?

If you answer yes to the first question plus at least one additional question, you are in a tactical environment and this overlay applies.

3. Implementation

<Insert the instructions for implementing the overlay.>

Guidance (delete when the guidance is completed): Define which revision of NIST SP 800-53 and CNSSI No. 1253 was used to develop the overlay.

Identify which baseline is the foundation for the overlay. Overlays that add security controls should begin with a foundation of the LLL baseline unless a different baseline is supported by the characteristics of the overlay. If a different baseline is selected, provide a rationale for using that baseline as the foundation for the overlay. When security controls are removed from the baseline, document the removal of the controls from the HHH baseline.

Define any requirements related to implementation such as any additional overlays that are expected to be used in conjunction with this overlay and any guidance that should be considered when tailoring the resulting set of security controls developed from the selected baseline and applicable overlays.

Security controls specified through the use of overlays can be implemented as a common, system-specific, or hybrid control based on organization-specific guidance.

Sample (delete when the description is completed):

The Privacy/HIPAA Overlay is based on:

- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009 with May 2010 errata updates
- CNSSI No. 1253, Revision 1.1, *Security Controls and Control Selections for National Security Systems*, Draft July 2011

The Privacy/HIPAA Overlay can apply to all the baselines defined in CNSSI No. 1253. Therefore, this overlay is developed based on the LLL baseline for any additional security control requirements. The overlay does not require any other overlays to provide the needed protection for systems containing privacy/ HIPAA information. Care should be taken when tailoring information systems that contain privacy/HIPAA information since numerous security controls are required by legislation. See Section 7 for the list of security controls required to meet regulatory/statutory requirements.

4. Table of Overlay Controls

<Insert a table with the security controls as they apply in this overlay.>

Guidance (delete when the security control table has been inserted): Identify the security controls that apply to the <Title> Overlay, using the format illustrated in Table 1. A plus sign ("+") in the overlay column indicates the applicability of the control above the controls identified in the 123 baseline. Two dashes ("--") in the overlay column indicates that the security control is not required and is effectively tailored from the final control set. Only the controls that differ from the selected baseline are included in the table. The table should include the: (i) control ID; and (ii) overlay controls.

It is possible to have an overlay without adding or subtracting security controls; the overlay may only include new supplemental guidance, parameter values, or regulatory/statutory controls.

If more than one type of information or more than one type of environment is associated with an overlay, multiple columns are used to document the different sets of security controls. For example, the Privacy/HIPAA overlay includes 3 columns representing 3 different control sets.

Table 1: <Insert Title> Overlay Security Controls

Sample (delete sample text and insert overlay-specific information):

CONTROL	<INSERT TITLE>	<INSERT TITLE>	<INSERT TITLE>
AC-2 (1)	--	--	
AC-2 (2)	--	--	
AC-2 (3)	--	--	
AC-3 (6)	+	+	+
AC-5	--		
AC-6 (3)	--	--	
AC-6 (5)	--	--	
AC-6 (6)	+		
AC-7	--		
AC-7 (2)	--	--	
AC-8	+	+	+
AC-9	--		
AC-10	--		
AC-14	+	+	+
AC-14 (1)	+	+	+

5. Supplemental Guidance

<Insert any supplemental guidance for the control selections in the overlay. If there is more than one set of security controls associated with an overlay (e.g., multiple RDT&E zones), provide separate supplemental guidance for each security control, as needed.>

Guidance (delete when the supplemental guidance is completed): In some cases, the supplemental guidance for the selected security controls and enhancements must be modified to address the characteristics of the overlays and the environments in which they operate. The supplemental guidance can also provide information as to why a particular security control or control enhancement may not be applicable in some environments and offer suggestions for compensating controls, as appropriate. The use of an overlay may also limit implementation options for some security controls. Therefore, the supplemental guidance may also include

implementation guidance for those controls. The overlay supplemental guidance should follow the format in NIST SP 800-53, Appendix I on Industrial Control Systems.

Sample 1 (delete when supplemental guidance is completed):

AC-3 ACCESS ENFORCEMENT

ICS Supplemental Guidance: The organization ensures that access enforcement mechanisms do not adversely impact the operational performance of the ICS.

References: NIST Special Publication 800-82

AC-8 SYSTEM USE NOTIFICATION

ICS Supplemental Guidance: In situations where the ICS cannot support system use notification, the organization employs appropriate compensating controls (e.g., posting physical notices in ICS facilities) in accordance with the general tailoring guidance.

CM-4 SECURITY IMPACT ANALYSIS

ICS Supplemental Guidance: The organization considers ICS safety and security interdependencies.

RA-2 SECURITY CATEGORIZATION

References: NIST Special Publication 800-82

6. Specific Value Parameters

<Insert any unique parameter values for the control selections in the overlay. If there is more than one set of security controls associated with an overlay, provide additional columns, as needed. If there are no unique parameter values for this overlay, state that in this section.>

Guidance (delete when the parameter values have been defined): An overlay should establish specific values as needed for the organization-defined parameters of the applicable controls; when those parameters did not have values specified for them in the CNSSI No. 1253 Appendix J specifications, or when the values for those parameters need to be different than those values identified for them in the applicable baseline or in any other overlays that are foundational for this overlay. Provide the specification of the appropriate values in a tabular format as shown below in sample Table 2, listing only those security controls for which the overlay needs to provide parameter values.

Table 2: Values for Parameters

Sample (delete sample text and insert overlay-specific information):

CONTROL	<INSERT TITLE>
AC-2 (2)	not to exceed 48 hours
AU-6	a. at least every 2 days

CONTROL	<INSERT TITLE>
CP-9 (1)	At least every 2 weeks
PE-2	c. at least every 6 months
SA-9 (1)	b. Chief Information Officer (CIO) and Risk Executive (Function)

7. Regulatory/Statutory Controls

<Insert the list of any security controls that are required on the basis of specific regulatory/ statutory requirements, if applicable, along with an identification of the specific regulatory/ statutory requirements. If none of the security controls are regulatory/statutory, state that in this section.>

Guidance (delete when the regulatory/statutory security controls have been defined): Some controls may be required for regulatory/statutory purposes. List those controls in a table as shown below in Table 3, listing only those security controls that are regulatory/statutory along with the identification of the specific requirement for the control.

Table 3: Regulatory/Statutory Security Controls

Sample (delete sample text and insert overlay-specific information):

CONTROL	<INSERT TITLE>	<INSERT TITLE>	<INSERT TITLE>
AC-1			45 CFR 164.308(a)(4)(i)
AC-2			45 CFR 164.308(a)(3)(ii)(A)
AC-3	5USC 552a(b), (e)(10)		45 CFR 164.308(a)
AC-3(6)		5USC 552a(e)(10)	45 CFR 164.312(a)(2)(iv)

8. Tailoring Considerations

<Insert any tailoring guidance related to the use of the overlay. If no tailoring guidance is needed, state that in this section.>

Guidance (delete when the tailoring guidance has been defined): An information system owner may need to tailor the set of security controls established by simply combining the baseline and all appropriate overlays. In some cases the use of multiple overlays may provide conflicting guidance. The authorizing official has the authority to approve the tailoring decisions and resulting set of security controls. While the information system owner, in conjunction with the authorizing official, determines the appropriate set of security controls for an information system, overlay developers may want to include information that will help guide those tailoring decisions.

Sample (delete when the overlay exceptions are completed):

When tailoring a security control set that includes the Privacy/HIPAA Overlay, care should be taken that regulatory/statutory security controls are not tailored from the control set. These security controls are required to satisfy the regulatory/statutory requirements of the Privacy Act or HIPAA. Failure to implement these security controls when privacy or health care information is included in the information system can result in fines up to $ and other civil penalties including loss of job or incarceration.

9. Duration

<Insert any the events that triggers an update to the overlay other than changes to NIST SP 800-53, CNSSI No. 1253, or DoD/IC security guidance. If there are no unique events that can trigger an update for this overlay, state that in this section.>

Guidance (delete when the events that trigger updates to the overlay have been defined): Identify the events that can cause the overlay to be modified or updated. Do not include changes in NIST SP 800-53 or CNSSI No. 1253 in this list. These documents serve as the foundation to the overlays and updates to those documents will automatically trigger events that will cause the overlays to be reviewed.

Sample (delete when the update events have been defined):

The overlay should be evaluated for revision when OMB issues new guidance that may impact designation of privacy or HIPAA-related security controls or if any of the following are revised: • The Privacy Act of 1974, as amended (The Privacy Act) • The Health Insurance Portability and Accountability Act of 1996 (HIPAA) • E-Government Act of 2002

10. Definitions

<Insert any definitions that are relevant to this overlay in alphabetical order. If there are no unique definitions for this overlay, state that in this section.>

Guidance (delete when the definitions have been defined): Define the terms that are unique to this overlay. The definitions are included in a word table to they can be sorted and formatted. After the definitions are complete, erase the lines (i.e., make them invisible), but keep the table (i.e., retain the table structure.

Sample (delete when the definitions have been documented):

Space Platform	An orbiting satellite, spacecraft, or space station developed, launched, and operated for purposes of providing specified products or services to users or customers. (CNSSP 12)
Space Station	All of the devices and organizations forming the space network. These consist of:

	spacecraft; mission package(s); ground stations; data links among spacecraft, ground stations; and mission or user terminals, which may include initial reception, processing, and exploitation; launch systems; and directly related supporting infrastructure, including space surveillance and battle management and/or command, control communications, and computers. (CNSSP 12)
Transmission Security (TRANSEC)	Measures (security controls) applied to transmissions in order to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals. (CNSSI 4009)