INTERAGENCY
SECURITY
COMMITTEE

Interagency Security Committee Compliance Policy and Compliance Benchmarks

Publication: January 2025

Cybersecurity and Infrastructure Security Agency

Change History and Document Control

Rev. #	Date	Changes	Approver
1.0	2016	Original document	ISC
2.0	2019	Updated document content extensively to capture lessons learned from Limited Rollout of the ISC Compliance Program	ISC
3.0	2024	Updated document title to include Compliance Policy and added new benchmark questions to align with 2024 ISC Risk Management Process Standard	ISC

Document Control

Distribution is authorized to federal, state, local agencies, and private individuals or enterprises.

Message from the Interagency Security Committee Chair

According to the 2024 Homeland Threat Assessment issued by the U.S. Department of Homeland Security, America continues to face a dynamic threat environment. To counter those threats, the Interagency Security Committee (ISC) advances efforts to mitigate risks to federal facilities through security best practices, policies, and standards.

In meeting the requirements of EO 14111 – *Interagency Security Committee,* to monitor agency compliance with ISC Policies and Standards, the ISC Compliance subcommittee developed the ISC benchmarks. The *Interagency Security Committee Compliance Policy and Benchmarks 2024 Edition* guides security planners in assessing the degree to which organizations and facilities have implemented ISC Policies and Standards.

These compliance benchmarks are modeled after the critical information found in the *Risk Management Process: An Interagency Security Committee Standard, Items Prohibited in Federal Facilities: An Interagency Security Committee Standard, and Planning and Response to an Active Shooter: An Interagency Security Committee Policy and Best Practices Guide.*

In addition, the guide helps organizations indicate key aspects of compliance with ISC Policies and Standards and the effectiveness or health of their security programs.

This document showcases the exceptional leadership of the Compliance Subcommittee and the collective collaboration of ISC members.

David Mussington, Ph.D., CISSP Associate C|CISO

Executive Assistant Director for Infrastructure Security

Cybersecurity and Infrastructure Security Agency

ISC Compliance Policy

Intent

The policy below establishes baseline department/agency protocols across the Federal Government for achieving compliance with ISC Policies and Standards. Executive Order (EO) 14111 requires the Interagency Security Committee (ISC) to "*develop a strategy to monitor the implementation of such standards to ensure compliance.*" This compliance policy is issued as part of that requirement and is applicable to those organizations and facilities to which EO 14111 applies.

Policy

1) Department and Agencies (Agencies) shall meet the annual ISC compliance reporting requirements by responding to benchmark questions for their organization and the facility(ies) they occupy.
2) Agencies shall have a program established to meet and report compliance with the ISC Policies and Standards. At a minimum, the program should comprise of the following elements:
   - A means to collect data directly correlated to the published ISC Compliance Benchmarks and to submit their agency compliance information into the ISC-Compliance System (ISC-CS) database.
   - Participate in ISC trainings to educate the appropriate staff (e.g., new ISC-CS administrators, uploaders, and viewers) on how to use the ISC-CS and meet the established reporting requirements.
   - Participate in a verification review when selected to validate their information reported in the ISC-CS.
     i. Identify appropriate staff to act as the verification point of contact.
     ii. Have a methodology to justify the compliance data reported (e.g., how to track deficiencies; perform document reviews to verify the data inputs).
     iii. Reach out to the ISC Compliance Team for assistance in reporting and validating compliance information as needed.
3) The ISC shall manage compliance reporting and verification, including:
   - Assist agencies by providing compliance training, training materials, and documentation to agency leadership and ISC-CS administrators, uploaders, and viewers as needed.
   - Prepare and provide the Director of the Office of Management and Budget and the Assistant to the President for National Security Affairs a summary report describing the results of compliance.
   - Administer a verification team who will work with selected agencies on the validation of their reported compliance information.
4) ISC members with validated compliance programs may be used, with agency approval, to provide mentoring and peer support to other ISC members directly.

Table of Contents

1.0 Introduction

Executive Order 14111 directs the Interagency Security Committee (ISC)[1] to "*evaluate existing security standards for Federal facilities and develop a strategy to monitor the implementation of such standards to ensure compliance by agencies*." Two of the duties carried out by the ISC to meet the requirements of EO 14111 are (1) monitoring agency compliance with ISC Policies and Standards and (2) developing and maintaining a centralized security database. Furthermore, EO 14111 does the following:

- Updates the definition of federal facilities to reduce ambiguity.
- Clarifies roles and responsibilities.
- Requires agencies to designate a Senior Official responsible for implementation of and compliance with the executive order and to support Facility Security Committees.
- Establishes minimum compliance monitoring requirements, to include conducting risk-based compliance verification.
- Requires the development of best practices for securing a mobile federal workforce.
- Directs the development of a biennial report detailing compliance results to the Director of the Office of Management and Budget and the Assistant to the President for National Security Affairs.

The primary mission of the ISC Compliance Subcommittee is to develop a strategy for ensuring compliance with established policies and standards and develop a strategy to monitor the implementation of such standards to ensure compliance by agencies. Monitoring compliance shall consist, at a minimum, of the following:

(i) maintaining compliance benchmarks to measure compliance progress;

(ii) requiring periodic compliance reporting by all relevant agencies; and

(iii) conducting risk-based compliance verification.

[1] The ISC was created by EO 12977, as amended by EO 13286 and EO 14111 to enhance the quality and effectiveness of security in, and protection of, buildings and facilities in the United States occupied by Federal employees for nonmilitary activities (Federal facilities), and to provide a permanent body to address continuing government-wide security for Federal facilities. ISC Standards apply to all civilian Federal facilities – whether government-owned, leased, or managed; or to be purchased.

2.0 Applicability and Scope

Pursuant to the Authority of the ISC in EO 14111, all federally owned or leased buildings, structures, and the land they reside on, in whole or in part, regularly occupied[2] by executive branch federal employees and/or federal contract workers for nonmilitary activities is subject to ISC Policies and Standards.[3]

Title 41, Code of Federal Regulations (CFR), Part 102-81, Physical Security is applicable to "federally owned and leased facilities and grounds under the jurisdiction, custody, or control of General Services Administration (GSA), including those facilities and grounds that have been delegated by the Administrator of General Services." In 2022, the GSA amended 41 CFR § 102-81.25 "to clarify that federal agencies are responsible for meeting physical security standards at nonmilitary facilities in accordance with ISC standards, policies, and recommendations."[4] Additionally, per DoD Instruction, 2000.12, all DoD leased facility space or space in buildings owned or operated by the GSA not located on DoD property must comply with this ISC Policies and Standards.

[2] The responsible authority determines "regularly occupied." For single-tenant facilities, a single office designated by the organization (e.g., Director of Security) may make occupancy determinations ensuring consistency across the organization. An occupied facility is when there is federal, or contract employees permanently or regularly assigned.

[3] The authority for Federal departments and agencies to provide security for their facilities and employees is cited in various sections of the United States Code (USC) and the Code of Federal Regulations (CFR). Nothing in these benchmarks supersedes those authorities. In accordance with their respective authority, each department or agency obtains the funds to provide security at its facilities. It is beyond the scope of this document to cite individual department and agency authorities. For more information regarding authorities, the reader should contact their agency's Office of General Counsel.

[4] See 87 FR 51915

3.0 Key Definitions

TERM	DEFINITION
Facility Security Level (FSL)	A categorization based on the analysis of several security-related facility factors, which serves as the basis for the identification of preliminary countermeasures and recurring risk assessments.
Level of Protection (LOP)	The degree of security provided by a particular countermeasure or set of countermeasures. Levels of protection used in the Risk Management Process Standard are Minimum, Low, Medium, High, and Very High.
Responsible Authority[5]	Facility Security Committee (FSC), tenant representative for single-tenant facilities, or legal authority (i.e., courtroom where a judge exercises authority).
Risk Acceptance	The explicit or implicit decision not to take an action that would affect all or part of a particular risk.
Risk Assessment	The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences.
Risk Management	A comprehensive approach to allocating resources for the protection of a facility, assets, and occupants to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and-when necessary-risk acceptance.
Senior Official	An organization's principle executive authority responsible for implementation and compliance with ISC Standards.

For a comprehensive list of definitions, refer to the Glossary of Terms.

[5] The definition of "Responsible Authority" does not include the term "Designated Official (DO)." 41 CFR § 102-74.230 establishes and defines specific responsibilities for the DO centered around the Occupant Emergency Program.

4.0 Benchmarks Organization

The Compliance Benchmarks are a mechanism to assess the degree to which federal agencies and their facilities have implemented the policies and standards of the ISC. They were written to correspond directly to the requirements set forth by *The Risk Management Process for Federal Facilities: An ISC Standard* (hereafter "the RMP"), *Items Prohibited from Federal Facilities: An ISC Standard*, and *Planning and Response to an Active Shooter: An ISC Policy and Best Practices Guide*. The benchmarks do not assess the application of individual countermeasures.

The benchmark questions are divided into three sections based on respondent: Organization Compliance Benchmarks, Facility Compliance Benchmarks, and Multi-Tenant Facility Compliance Benchmarks. The Organization Compliance Benchmark questions will be filled out at the sub-organization/agency/bureau level. The Facility Compliance Benchmark questions will be filled out for each facility (both single and multi-tenant) leased or owned by the organization or under an occupancy agreement. The Multi-Tenant Facility Compliance Benchmark questions will be completed only for multi-tenant facilities leased or owned by the organization or under an occupancy agreement. These three sections are further divided into subsections that correspond to a specific topic/area within the ISC Policies and Standards.

Within each subsection is a set of primary benchmark questions and supporting benchmark questions. The primary benchmarks indicate key aspects of compliance with ISC Policies and Standards. The supporting benchmarks provide information on the effectiveness or health of the corresponding security programs/procedures.

5.0 Roles and Responsibilities

1. Agencies shall establish and maintain a program to ensure compliance with ISC Policies and Standards.[6] The program may be centralized or decentralized.
2. Agencies shall report compliance benchmark responses to the ISC associated with the implementation of ISC Policies and Standards across their organization (7.0-Section 1).
3. Agencies shall report compliance benchmark responses to the ISC associated with all leased or owned facilities they occupy, and ensure that all facilities are evaluated against the current ISC Compliance Benchmarks:
    a. For those facilities where the agency is the sole federal tenant, the facility will be evaluated against the single-tenant benchmarks found in 7.0-Section 2 of the benchmarks and report those results to the ISC.
    b. For those facilities with multiple federal tenants, the facility will be evaluated against the benchmarks found in 7.0-Section 2 and 7.0-Section 3; and each tenant agency shall report those results to the ISC.
4. Agencies shall certify ISC compliance and associated metrics/information using a standard automated form (electronic submissions).
5. The ISC shall issue guidance to agencies to assist with efforts to oversee compliance with ISC Policies and Standards. Guidance documents will include organizational level requirements/standards and facility-specific requirements/standards.
6. The ISC shall develop and maintain an automated database for tracking individual agency submissions and compliance metrics.
7. The ISC shall monitor agency compliance at the organizational and facility levels through yearly analysis, assistance, and a risk-based verification program.
8. All occupants of multi-tenant facilities shall report individually through their agency headquarters benchmarks that have been coordinated with the Facility Security Committee for that facility.

[6] In the instances where more restrictive agency-specific security policies are employed in lieu of ISC Standards, the organization is still responsible for verifying compliance with ISC Standards using the Compliance Benchmarks and submitting associated metrics/information.

6.0 Likert Scale Response Explanations

The below tables represent the responses that organizations will use to answer the various benchmark questions. The scales provide the ability for the ISC to understand how organizations are complying based on status of progress, comparison, frequency, percentage, and time. The tables listed as "Supporting" are used in responses to Supporting Benchmark Questions only and include an "N/A" or "0" field. Those responding to the benchmark questions should utilize these descriptions before making their response selection.

Table 1: Status

Question: What is the status of _____?	
Likert Scale	**Description of Response**
Not Started	In planning stage but not yet begun – or – has not occurred at time of reporting
Initiated	Begun but not progressed
In Process	Well underway
Nearing Completion	Under review prior to completion
Complete	Developed, approved, issued, distributed, and implemented

Table 2: Comparison

Question: How does _____ compare?	
Likert Scale	**Description of Response**
Not at All	The item does not meet any of the standards
Partially	The item meets few of the standards
Somewhat	The item meets some of the standards
Mostly	The item meets most of the standards
Same	The item meets or exceeds all the standards

Table 3: Frequency

Question: What is the frequency of _____? How often does _____ occur?	
Likert Scale	**Description of Response**
Never	Never
Sometimes	Approximately 25% of the time
Often	Approximately 50% of the time
Usually	Approximately 75% of the time
Always	Happens 100% of the time

Table 4: Percentage

Question: What is the percentage of _____?	
Likert Scale	**Description of Response**
0%	No more than 0%
1-33%	Greater than 0% but no more than 33%
34-66%	Greater than 33% but no more than 66%
67-99%	Greater than 66% but less than 100%
100%	No less than 100%

Table 5: Years

Question: How many years does _____?	
Likert Scale	**Description of Response**
0 years	Less than 1 year
1-3 years	At least 1 year and less than 4 years
4-6 years	At least 4 years and less than 7 years
7-9 years	At least 7 years and less than 10 years
10+ years	Greater than or equal to 10 years

Table 6: Plan Components

Question: Does the plan incorporate roles and responsibilities?	
Likert Scale	**Description of Response**
Plan Does Not Address	Plan does not incorporate any roles or responsibilities
Developing	Definition of roles and responsibilities is well underway
Some Roles and Responsibilities Defined	Some roles and responsibilities are defined, but have not been reviewed and/or approved
Nearing completion	All roles and responsibilities are defined and under review prior to completion
All Roles and Responsibilities Defined	Roles and responsibilities are developed, approved, issued, distributed, and implemented

Table 7: Active Shooter Plan Exercise Frequency

Question: How often is the active shooter preparedness plan exercised?	
Likert Scale	**Description of Response**
Never	Plan does not exist and/or has not been exercised
Every 3 years or greater	It has been longer than three years since the last exercise
Greater than 2 years, less than 3 years	It has been between two and three years since the last exercise
Greater than 1 year, less than 2 years	It has been between one and two years since the last exercise
Annually	The plan is exercised every year in some manner (e.g., tabletop, functional, full-scale).

Table 8: FSC Meetings

Question: How often does the FSC meet?	
Likert Scale	**Description of Response**
Never	The FSC has never met
Once Every Three Years	The FSC has met no more than one time in the past three years
Once Every Two Years	The FSC has met no more than one time in the past two years
Once Every Year	The FSC has met no more than one time in the past year
At Least Twice Per Year	The FSC has met two or more times in the past year

Table 9: Comparison – Supporting Benchmarks

Question: How does ______ compare?	
Likert Scale	**Description of Response**
N/A	This question is not applicable to the Agency
Not at All	The item does not meet any of the standards
Partially	The item meets few of the standards
Somewhat	The item meets some of the standards
Mostly	The item meets most of the standards
Same	The item meets or exceeds all the standards

Table 10: Frequency – Supporting Benchmarks

Question: What is the frequency of _______? How frequently does ________ occur?	
Likert Scale	**Description of Response**
N/A	This question is not applicable to the Agency
Never	Never
Sometimes	Approximately 25% of the time
Often	Approximately 50% of the time
Usually	Approximately 75% of the time
Always	Happens 100% of the time

Table 11: Percentage – Supporting Benchmarks

Question: What is the percentage of ______?	
Likert Scale	**Description of Response**
0%	No more than 0%
1-24%	Greater than 0% but no more than 24%, approximately
25-49%	Greater than 24% but no more than 49%, approximately
50-74%	Greater than 49% but no more than 74%, approximately
75-99%	Greater than 74% but less than 100%, approximately
100%	No less than 100%

Table 12: Status – Supporting Benchmarks

Question: What is the status of ______?	
Likert Scale	**Description of Response**
Not Started	Has not occurred at time of reporting
Planned	In planning stage but not yet begun
Initiated	Begun but not progressed
In Process	Well underway
Nearing Completion	Under review prior to completion
Complete	Developed, approved, issued, distributed, and implemented

7.0 Benchmarks

Section 1: Organization Compliance Benchmarks

1.1 Organization ISC Implementation Guidance

Individual organizations shall document and issue guidance throughout their organization which requires compliance with ISC Policies and Standards.

1.1.1 Primary Benchmarks

1. What is the status of your organization's policy or guidance to comply with the ISC Policies and Standards for applicable occupied facilities pursuant to EO 14111?

1=Not Started	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 3.0

2. What percentage of your facilities has your organization issued a policy to instructing them to comply with ISC Policies and Standards?

1=0%	2=1-33%	3=34-66%	4=67-99%	5=100%
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 3.0

3. What is the status of your organization assigning a Senior Official to be responsible for the implementation of ISC Policies and Standards?

1=Not Started	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O

Reference: *RMP, 2024 Edition*, Section 5.1

1.1.2 Supporting Benchmarks

1. If your organization has developed its own risk management process, to what degree is it in line with ISC guidance to be credible, reproducible, defensible? *(Whereas defensible refers to both having a justification for any deviation from the enumerated baseline threat ratings found in "Appendix A: Design Basis Threat Report" AND correlates directly to the levels of protection found in "Appendix B: Countermeasures")*

N/A	1=Not at All	2=Partially	3=Somewhat	4=Mostly	5=Same
O	O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.2.1 & 8.2.2

2. What is the status of development of your organization's process to document risk acceptance?

Not Started	1=Planned	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
○	○	○	○	○	○

Reference: *RMP, 2024 Edition,* Section 5.3 & 8.4.2

1.2 Utilization of the ISC Risk Management Process

Evaluates organization compliance with the security standards established in the most recent version of the RMP.

1.2.1 Primary Benchmarks

1. What percentage of your facilities have a Facility Security Level (FSL) determination?

1=0%	2=1-33%	3=34-66%	4=67-99%	5=100%
○	○	○	○	○

Reference: *RMP, 2024 Edition,* Section 8.1.1

2. What percentage of your facilities have had a risk assessment conducted in accordance with ISC-directed intervals?

1=0%	2=1-33%	3=34-66%	4=67-99%	5=100%
○	○	○	○	○

Reference: *RMP, 2024 Edition*, Section 8.1.1

3. What percentage of your organization's facilities does your organizational security element track and maintain documented risk acceptance decisions pursuant to the RMP?

1=0%	2=1-33%	3=34-66%	4=67-99%	5=100%
○	○	○	○	○

Reference: *RMP, 2024 Edition*, Sections 5.3, 8.3.1 & 8.4.2

4. How often does the risk assessment methodology utilized at your organization's facilities meet, or exceed, the standards to be credible, reproducible, defensible? *(Whereas defensible refers to both having a justification for any deviation from the enumerated baseline threat ratings found in "Appendix A: Design Basis Threat Report" AND correlates directly to the levels of protection found in "Appendix B: Countermeasures")*

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
○	○	○	○	○

Reference: *RMP, 2024 Edition,* Section 8.2.1 & 8.2.2

5. How often does the security organization use *Appendix A: Design-Basis Threat (DBT) Report*, or other threat assessment that meets or exceeds the standards set in the DBT, to support the calculation of facility risk (threat, vulnerability, consequence) when determining the necessary level of protection (LOP)?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix A: The Design-Basis Threat Report*

6. What is the status of your organization's routine communication with the responsible authority for each federal facility?

1=Not Started	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee*, Section D.1

7. What percentage of your organization's FSC representatives or responsible authority for single tenant facility have completed mandated training?

1=0%	2=1-33%	3=34-66%	4=67-99%	5=100%
O	O	O	O	O

Reference: *RMP, 2024 Edition*, Section 6.0 *& Appendix D: How to Conduct a Facility Security Committee*, Section D.2.

8. What percentage of unmitigated risk across your facility portfolio is addressed by annual budget submissions?

1=0%	2=1-33%	3=34-66%	4=67-99%	5=100%
O	O	O	O	O

Reference: *RMP, 2024 Edition*, Section 5.2 & 7.0

9. How often does the Organizational Security Element or Senior Official provide voting and funding guidance; guidance on security policy and risk management strategies; and compliance initiatives to responsible authorities in response to risk assessments?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition*, Section 5.2 & 5.3

10. What's the status of your organization implementing its risk register to document and track accepted risk within your facility portfolio?

1=Not Started	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O

Reference: *RMP*, *2024 Edition*, Section 5.3 & 7.2

11. What is the status of your organization implementing a security performance measurement and testing program?

1=Not Started	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O

Reference: *RMP*, *2024 Edition*, Section 5.3 & 8.5*; Appendix E: Use of Performance Security Measures,* Section E.1

1.2.2 Supporting Benchmarks

1. Approximately what percentage of ISC compliance benchmarks are verified by your organization's headquarters?

0%	1=1-24%	2=25-49%	3=50-74%	4=75-99%	5=100%
O	O	O	O	O	O

Reference: *RMP*, *2024 Edition*, Section 5.1

2. What is the status of your organization's policy or guidance that assists responsible authorities to address and resolve issues?

Not Started	1=Planned	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O	O

Reference: *RMP, 2024 Edition*, Section 5.2 *& Appendix D: How to Conduct a Facility Security Committee*, Section D.4.2

3. Approximately what percentage of facilities operating under your organization's authority use the RMP?

N/A	1=0-24%	2=25-49%	3=50-74%	4=75-99%	5=100%
O	O	O	O	O	O

Reference: *RMP*, *2024 Edition*, Section 3.0

4. What percentage of your facilities does your organization maintain records, inspection reports, and metrics for in support of its performance measurement program?

N/A	1=0-24%	2=25-49%	3=50-74%	4=75-99%	5=100%
O	O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.5, *& Appendix E: Use of Performance Security Measures,* Section E.3

5. What is the status of maintaining a current list of federal facilities occupied by the organization to include FSL (or equivalent) designations?

Not Started	1=Planned	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 5.3 *& Appendix E: Use of Performance Security Measures,* Section E.3

6. What percentage of your facilities do you maintain communication with on a regular basis concerning ISC Policies and Standards?

N/A	1=0-24%	2=25-49%	3=50-74%	4=75-99%	5=100%
O	O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 5.3 *& Appendix E: Use of Performance Security Measures,* Section E.3

7. What's the status of your organization maintaining a roster of FSC Chairs, Representatives, or Responsible Authority at all occupied facilities?

Not Started	1=Planned	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 5.3

8. How often does your organization assess the implementation of the security organization's identified countermeasures required to meet the necessary or achievable LOP from the latest risk assessment?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.4 & 8.5

9. What percentage of facilities that your organization occupies have achieved the Necessary LOP as determined from their most recent risk assessment OR have formally accepted risk and meet the achievable LOP?

1=0%	2=1-33%	3=34-66%	4=67-99%	5=100%
O	O	O	O	O

Reference: *RMP*, *2024 Edition*, Section 8.3

Section 2: Facility Compliance Benchmarks

2.1 Application of a Risk Management Process

Evaluation of the facility's application of the RMP.

2.1.1 Primary Benchmarks

1. How often does your facility use procedures that meet or exceed those defined in the RMP (or equivalent process) to assess facility risk, determine which security countermeasures are implemented, and what level of risk is accepted?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 3.0

2. How often does your facility security organization conduct risk assessments in accordance with the FSL (or similar security level determination) contingent timeframe identified in the RMP (or equivalent process)?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.1.1 (RMP – Step 1)

3. How often are the following factors used to determine your facility's FSL (or similar security level determination): mission criticality, symbolism, facility population, facility size, threat to tenant organization, and intangible adjustments?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.1.3 (RMP – Step 1)

4. How often are all of the applicable undesirable events in the DBT, or other threat source that meets or exceeds the DBT, evaluated when identifying and assessing risk at the facility?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix A: The Design-Basis Threat Report (FOUO),* Section 7.0 (RMP – Step 2)

5. What is the status of your facility's security organization providing a final risk assessment report to the responsible authority for proposed countermeasures that identifies how it will mitigate the risks identified with specific credible threats since your facility’s last security assessment?

1=Not Started	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O

Reference: *RMP, 2024 Edition, Section 8.2.4* (RMP – Step 2)

6. If the responsible authority determines that it cannot implement the necessary LOP, how often do they identify the highest achievable LOP?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.3.2. (RMP – Step 3)

7. If the existing LOP does not meet the necessary LOP, how often does the security organization identify the difference between the LOPs and the countermeasures necessary to mitigate existing vulnerability?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.3 (RMP – Step 3)

8. How often does your facility document the accepted risk, including alternate strategies considered or implemented, if the necessary level of protection (LOP) cannot be achieved?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.4.2 (RMP – Step 4)

9. How often, when risk is identified but the permanent countermeasures to mitigate it are not immediately achievable, are interim countermeasures considered, including a plan for future permanent replacement?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.4.4 (RMP – Step 4)

10. How often does the responsible authority receive countermeasures testing results from the security organization for this facility?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.5.1 (RMP – Step 5)

11. How often does the owning or leasing authority or security organization provide the necessary information to fund security countermeasure projects?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Sections 5.4 and 7.3

12. What is the status of the facility's responsible authority receiving organizational policy or guidance to follow the ISC's Risk Management Process?

1=Not Started	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 5.1

2.1.2 Supporting Benchmarks

1. What is the status of the responsible authority establishing an FSL in collaboration with the security organization, the owning or leasing authority, and other appropriate stakeholders?

Not Started	1=Planned	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.1.1

2. How often are short-term events at the facility addressed through contingency plans to implement temporary countermeasures until the event has passed (e.g., week-long conference that temporarily increases the facility population, but is not a continuous event that would impact the FSL)?

N/A	1=Never	2= Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.1.3

3. If an overall campus FSL has been designated for multiple facilities, how often is the campus FSL calculated using the highest rating of any tenant in the campus for each FSL determination factor?

N/A	1=Never	2= Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.1.5

4. How often does your facility security organization review the FSL when there are changes such as tenant composition or the mission performed in the facility?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.1.6

5. How often does the security organization provide the information necessary for decision making on identified countermeasures required to achieve the necessary LOP to the responsible authority (including threat, vulnerability, consequence, and cost)?

N/A	1=Never	2= Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.2.4

6. What percentage of identified countermeasures from the most recent risk assessment have been approved?

0=0%	1=1-24%	2 = 25-49%	3=50-74%	4=75-99%	5=100%
O	O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.3 & 8.4

7. What percentage of approved countermeasures from the most recent risk assessment have been implemented at your facility to achieve the necessary LOP?

0=0%	1=1-24%	2 = 25-49%	3=50-74%	4=75-99%	5 = 100%
O	O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 8.3 & 8.4

8. How often does the responsible authority retain important records/reports of assessments in accordance with the RMP?

1=Never	2= Sometimes	3=Often	4=Usually	5=Always
○	○	○	○	○

Reference: *RMP, 2024 Edition*, Section 8.5*; Appendix D: Facility Security Committee Procedures; Appendix E: Security Performance Measures*

9. What percentage of testable countermeasures at the facility are evaluated with performance measures to monitor the effectiveness and reduction of overall risk to the facility?

N/A	1=0-24%	2=25-49%	3=50-74%	4=75-99%	5=100%
○	○	○	○	○	○

Reference: *RMP, 2024 Edition, Appendix E: Use of Performance Security Measures*, Section E.2.1

10. If the facility contains a child-care center, how often is the director of the child-care center included in the risk management process as a non-voting member?

N/A	1=Never	2= Sometimes	3=Often	4=Usually	5=Always
○	○	○	○	○	○

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee, Section D.3*

2.2 Implementation of *Planning and Response to an Active Shooter: An ISC Policy and Best Practices Guide*

Evaluation of the facility's development and implementation of the requirements outlined in the ISC's *Planning and Response to an Active Shooter: An ISC Policy and Best Practices Guide*.

2.2.1 Primary Benchmarks

1. What is the status of your facility's active shooter preparedness plan that contains the elements of: pre-incident planning; incident actions; and post-incident recovery as defined by ISC Policy?

1=Not Started	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
○	○	○	○	○

Reference: *Planning and Response to an Active Shooter*, Section ISC Policy

2. What is the status of your facility reviewing and, if necessary, updating its active shooter preparedness plan annually?

1=Not Started	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O

Reference: *Planning and Response to an Active Shooter,* Section ISC Policy

3. How often does your facility coordinate with applicable facility security organization and/or first responders during development of the active shooter preparedness plan?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *Planning and Response to an Active Shooter,* Section ISC Policy

4. How often does your facility collaborate with all facility tenants/agencies during development of the active shooter preparedness plan?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *Planning and Response to an Active Shooter,* Section ISC Policy

5. How often does your facility train its employees on the federally endorsed “Run, Hide, Fight” concept?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *Planning and Response to an Active Shooter,* Section ISC Policy

6. How often does your facility train employees on the facility level active shooter preparedness plan in accordance with ISC Policy from the point of onboarding and annually thereafter?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *Planning and Response to an Active Shooter,* Section ISC Policy

7. How often does your facility inform all of its employees on the importance of having a personal plan?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *Planning and Response to an Active Shooter,* Section ISC Policy

8. To what extent does your facility's active shooter preparedness plan incorporate the roles and responsibilities of security and law enforcement personnel identified through collaboration with the same?

1=Plan Does Not Address	2=Developing	3=Some Roles and Responsibilities Defined	4=Nearing Completion	5=All Roles and Responsibilities Defined
O	O	O	O	O

Reference: *Planning and Response to an Active Shooter,* Section ISC Policy

9. How often is the active shooter preparedness plan exercised (e.g., tabletop, functional, full-scale, etc.)?

1=Never	2= Every 3 years or greater	3= Greater than every 2 years, but less than every 3 years	4= Greater than every 1 year, but less than every 2 years	5=Annually
O	O	O	O	O

Reference: *Planning and Response to an Active Shooter,* Section ISC Policy

10. What is the status of your facility's responsible authority receiving organizational policy or guidance to follow the Active Shooter Policy?

1=Not Started	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 5.3

2.3 Implementation of *Items Prohibited from Federal Facilities: An ISC Standard*

Evaluation of the facility's implementation of the established baseline list of prohibited items.

2.3.1 Primary Benchmarks

1. What is the status of your facility having a facility-specific codified list of prohibited items that is reviewed annually?

1=Not Started	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O

Reference: *Items Prohibited from Federal Facilities: An ISC Standard,* Section 5.0; 18 U.S.C. § 930

2. What is the status of your responsible authority having a procedure for exemptions and exceptions for prohibited items?

1=Not Started	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O

Reference: *Items Prohibited from Federal Facilities: An ISC Standard,* Section 6.0

3. How often does your responsible authority provide a copy of all approved exceptions and exemptions to each screening checkpoint and to the facility security organization or to appropriate staff when updates or changes are made?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *Items Prohibited from Federal Facilities: An ISC Standard,* Section 6.2

4. What percentage of all public-facing entrances have a notice of prohibited items posted?

1=0%	2=1-33%	3=34-66%	4=67-99%	5=100%
O	O	O	O	O

Reference: *Items Prohibited from Federal Facilities: An ISC Standard,* Section 5.0

5. What is the status of the responsible authority establishing procedures for the introduction and possession of controlled items?

1=Not Started	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O

Reference: *Items Prohibited from Federal Facilities: An ISC Standard,* Section 7.0

6. What is the status of your facility's responsible authority receiving organizational policy or guidance to implement the Prohibited Items Standard?

1=Not Started	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O

Reference: *RMP, 2024 Edition,* Section 5.1

Section 3: Multi-Tenant Facility Compliance Benchmarks

3.1 Facility Security Committees

Evaluation of the administration of the FSC for multi-tenant facilities.

3.1.1 Primary Benchmarks

1. If your facility has two or more Federal tenants, what is the status of the establishment of an FSC with a formal charter?

1=Not Started	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee,* Section D.1

2. How often does the FSC meet?

1=Never	2=Once Every Three Years	3=Once Every Two Years	4=Once Every Year	5=At Least Twice Per Year
O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee,* Section D.3.3

3. How does the FSC's voting procedure compare with ISC Standards set in the RMP?

1=Not at all	2=Partially	3=Somewhat	4=Mostly	5=Same
O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee,* Section D.3.5

4. How often are meeting minutes (to include FSC decisions) disseminated to FSC members?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee,* Section D.5

5. How often does the FSC use the appropriate process (Business, Funding, or Decision) to facilitate a final decision?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee,* Section D.4 through D.4.2

6. How often are your decision items voted on by a quorum of at least 50% of FSC tenant organizations, representing at least 51 percent of the RSF (rentable square feet)?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee,* Section D.3.5

3.1.2 Supporting Benchmarks

1. What is the status of the selection of the FSC chairperson?

Not Started	1=Planned	2=Initiated	3=In Process	4=Nearing Completion	5=Complete
O	O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee,* Section D.2.1

2. How often does the FSC chairperson establish the voting date on decision items within 45 calendar days of FSC members receiving all requested documents and materials?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee,* Section D.3.5

3. How often do FSC members have decision-making/funding authority for FSC decision items?

N/A	1=Never	2= Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee,* Section D.2.1

4. On average, approximately what percentage of federal tenant agencies participate in FSC meetings and decisions/votes?

N/A	1=0-24%	2=25-49%	3=50-74%	4=75-99%	5=100%
O	O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee,* Section D.3

5. What percentage of FSC members receive timely support, advice, and guidance from their organization headquarters when requested? (percentage question, if 7 out of 10 members, it is 70%).

N/A	1=0-24%	2=25-49%	3=50-74%	4=75-99%	5=100%
O	O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee,* Section D.2

6. What percentage of FSC members inform their organization headquarters of FSC activities and security issues at their facility, by providing meeting minutes, funding decisions, and/or risk acceptance to their respective headquarters?

N/A	1=0-24%	2=25-49%	3=50-74%	4=75-99%	5=100%
O	O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee,* Section D.2.1

7. How often do FSC members with RSF occupy their seat on the FSC, attend meetings, and vote in FSC matters?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee,* Section D.3

8. How often are FSC meeting minutes maintained by the FSC chairperson and the security organization as historical documents for the facility?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee,* Section D.5

9. How often does the security organization provide written funding requirements to all FSC members when presenting countermeasures plans to the FSC?

1=Never	2=Sometimes	3=Often	4=Usually	5=Always
O	O	O	O	O

Reference: *RMP, 2024 Edition, Appendix D: How to Conduct a Facility Security Committee,* Section D.3.6.1

8.0 Resources

8.1 List of Abbreviations/Acronyms/Initialisms

Abbreviation	**Full Name of Term**
CISA	Cybersecurity and Infrastructure Security Agency
CFR	Code of Federal Regulations
DBT	Design-Basis Threat
DHS	Department of Homeland Security
DO	Designated Official
DoD	Department of Defense
EO	Executive Order
FOUO	For Official Use Only
FSC	Facility Security Committee
ISC	Interagency Security Committee
ISC-CS	Interagency Security Committee Compliance System
LOP	Level of Protection
RMP	The Risk Management Process for Federal Facilities: An ISC Standard
RSF	Rentable Square Footage
USC	United States Code

8.2 Glossary of Terms

Term	Definition
Agency	An executive agency, as defined in section 105 of title 5, United States Code.
Building	An enclosed structure (above or below grade).
Campus	Two or more federal facilities contiguous and typically sharing some aspects of the environment, such as parking, courtyards, private vehicle access roads, or gates and entrances to connected buildings. A campus also may be a "federal center" or "complex."
Customized Level of Protection	The final set of countermeasures developed as the result of the risk-based analytical process.
Existing Federal Facility	A facility for which the design and construction effort has reached a stage where design changes may be cost prohibitive.
Existing Level of Protection	The degree of security provided by the set of countermeasures determined to be in existence at a facility.
Facility	Space built or established to serve a particular purpose. The facility is inclusive of a building or suite and associated support infrastructure (e.g., parking or utilities) and land.
Facility Security Committee	A committee that is established in accordance with an Interagency Security Committee standard, and that is responsible for addressing facility-specific security issues and approving the implementation of security measures and practices in multi-tenant facilities.
Facility Security Level	A categorization based on the analysis of several security-related facility factors, which serves as the basis for the identification of preliminary countermeasures and recurring risk assessments.
Federal Contractor Worker	Any individual who performs work for or on behalf of any agency under a contract, subcontract, or contract-like instrument and who, in order to perform the work specified under the contract, subcontract, or contract-like instrument, requires access to space, information, information technology systems, staff, or other assets of the Federal Government in buildings and facilities of the United States.
Federal Employee	An employee, as defined in section 2105 of title 5, United States Code, of an agency.
Federal Facility	A federally owned or leased building, structure, or the land it resides on, in whole or in part, that is regularly occupied by Federal employees or Federal contractor workers for nonmilitary activities. The term "Federal facility" also means any building or structure acquired by a contractor through ownership or leasehold interest, in whole or in part, solely for the purpose of executing a nonmilitary federal mission or function under the direction of an agency. The term "Federal facility" does not include public domain land, including improvements thereon; withdrawn lands; or buildings or facilities outside of the United States.

Term	Definition
Facility Security Assessment	The process and final product documenting an evaluation of the security-related risks to a facility. The process analyzes potential threats, vulnerabilities, and estimated consequences culminating in the risk impacting a facility using a variety of sources and information.
Federal Tenant	An agency that pays rent on space in a federal facility. See also: Single-tenant, multi-tenant, and mixed-multi-tenant.
Level of Protection	The degree of security provided by a particular countermeasure or set of countermeasures. Levels of protection used in the Risk Management Process Standard are Minimum, Low, Medium, High, and Very High.
Mixed-Tenant Facility	A facility that includes exactly one federal tenant as well as one or more non-federal tenants (including commercial and state, local, tribal, and territorial tenants).
Mixed-Multi-Tenant Facility	A facility that includes tenants from multiple agencies AND at least one non-federal tenant.
Multi-Tenant Facility	A facility that includes tenants from multiple agencies but no non-federal tenants.
Necessary Level of Protection	The determined degree of security needed to mitigate the assessed risks at the facility.
Nonmilitary Activities	Any facility not owned or leased by the Department of Defense.
Occupant	Any person regularly assigned to federally occupied space who has been issued and presents the required identification badge or pass for access. In multi-tenant facilities, the FSC establishes the thresholds for determining who qualifies for "occupant" status. Based on varying mission assignments, agencies have the flexibility to determine what constitutes a "regularly assigned" person.
Organizational Security Element	A headquarters or field component of a facility tenant's internal security office, or equivalent.
Owning or Leasing Authority	Entity authorized to enter into a lease agreement with a person, co-partnership, corporation, or other public or private entity for the accommodation of a federal agency in a facility.
Responsible Authority	Facility Security Committee (FSC), tenant representative for single-tenant facilities, or legal authority (i.e., c courtroom where a judge exercises authority).
Risk Acceptance	The explicit or implicit decision not to take an action that would affect all or part of a particular risk.
Risk Assessment	The process of evaluating credible threats, identifying vulnerabilities, and assessing consequences.

Term	Definition
Risk Management	A comprehensive approach to allocating resources for the protection of a facility, assets, and occupants to achieve an acceptable level of risk. Risk management decisions are based on the application of risk assessment, risk mitigation, and-when necessary-risk acceptance. Extended definition: Process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost. Annotation: The primary goal of risk management is to reduce or eliminate risk through mitigation measures (avoiding the risk or reducing the negative effect of the risk), but also includes the concepts of acceptance and/or transfer of responsibility for the risk as appropriate. Risk management principles acknowledge risk is difficult to eliminate; however, it is usually possible to take actions to reduce it.
Risk Management Methodology	A set of methods, principles, or rules used to identify, analyze, assess, and communicate risk, and mitigate, accept, or control it to an acceptable level at an acceptable cost.
Risk Register	A repository of risk information including the data understood about risks over time. Extended definition: A central record of current risks, and related information, for a given scope or organization. Current risks comprise both accepted risks and risks that have a planned mitigation path
Security Organization	The government agency or an internal agency component either identified by statute, interagency memorandum of understanding /memorandum of agreement, or policy responsible for physical security for the specific facility and performs preliminary FSL determinations and initial or recurring risk assessments.
Senior Official	An organization's principle executive authority responsible for implementation and compliance ISC Standards.
Single-tenant Facility	A facility that has exactly one federal tenant and zero non-federal tenants. This may include multiple components of a single agency.

8.3 References Cited

General Services Administration

- Title 41 CFR, part 102-81, Physical Security

Interagency Security Committee

- Federal Register: EO 14111-Interagency Security Committee
- Risk Management Process
- Prohibited Items
- Active Shooter

Acknowledgments

Compliance Subcommittee Participants

ISC Subcommittee Members

David Adams
Chief, Physical Security Branch
NARA

Gean Alston
Policy Advisor
DHS

Robert Daul
Information Security Programs Manager
CISA

Michael Griffin
Deputy Director, Physical Security Division
GSA

Luther Israel
Security Specialist
CISA

Glenn Kollar
Security Specialist
CISA

Jeff Levine
Special Agent in Charge
FPS

Robert Marston
DCSA

Kevin McCombs
Director
EPA

William "Carson" McHale
Office of Infrastructure Protection
FAA

Dennis Ouellette
Technical Advisor, Security
IRS

Frank Quintana
Supervisory Physical Security Specialist
HHS

John Rossiter
Security Specialist
SEC

Renee Speare
Physical Security Specialist
IRS

Natasha Sumter
Office of Security
DOE

Cybersecurity and Infrastructure Security Agency
Interagency Security Committee Staff Support

Daryle Hernandez, Chief

Deana Russo
Compliance Subcommittee Chair

Shawn Fiebiger
Deputy Compliance Program Manager

Robert Chaiet
Technical Editor

Kevin Choate
ISC Regional Advisor, Regions 6 and 8

Christopher York
Policy Analyst

Scott Dunford
Security Specialist

Tarvis Bonner
Program Analyst

David Hooker
Program Analyst