Department of Homeland Security
DHS Directives System
National Security Systems Policy Standard Number: 4300B.103-2
Version Number: 9.0
Issue Date: April 19, 2013

Template for Risk Assessment Reports

I. Purpose

This Standard provides the guidance and template for a Risk Assessment Report (RAR) for Department of Homeland Security (DHS) National Security Systems (NSS). A RAR provides an overview of the security of an information system and describes the controls and critical elements in place or planned for, based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Guide to Conducting Risk Assessments*.

II. Scope

This Standard applies to all DHS elements, employees, contractors, detailees, others working on behalf of DHS, and users of DHS NSS that collect, generate, process, store, display, transmit, or receive Confidential, Secret, or Top Secret classified national security information. These NSS include networks, information systems, standalone systems, and applications for which DHS is responsible and has authority, regardless of the physical location.

III. Policy

A. Completion of RARs is in support of NIST Special Publication 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, and Committee on National Security Systems (CNSS) Policy (CNSSP) 22, *Policy on Information Assurance Risk Management for National Security Systems*.

B. The RAR documents the results of planning and implementing adequate, cost-effective security protection for a system. It reflects input from management

responsible for the system, including the Information System Owner (ISO), Information Owners (IO)/Stewards, the system operator, the Information System Security Manager (ISSM), and system administrators (SA).

C. The RAR is based upon a review of the environment, documentation, DHS regulations/guidance, and interviews with the information system personnel conducted between certain identified dates. The RAR includes the results of planning and implementing adequate, cost-effective security protection for a system.

IV. References

For a listing of references that apply to DHS NSS, refer to DHS NSS Policy Standard 4300B.108-1, *National Security System References*.

V. Definitions

Definitions specific to NSS are defined in CNSS Instruction (CNSSI) 4009*, National Information Assurance Glossary*. The terms, as defined in CNSSI 4009, "safeguarding," "information security," and "information assurance" may be used interchangeably throughout this Standard.

VI. Responsibilities

Refer to NSS Policy Directive 4300B.100, *Safeguarding and Risk Management for National Security Systems*, Enclosure 2, for organization-wide roles and responsibilities for NSS. For responsibilities specific to steps within the Risk Management Framework (RMF) as applied to DHS, refer to NSS Policy Instruction 4300B.101, *Risk Management Framework for National Security Systems*.

VII. Processes and Procedures

A. A RAR documents the risk assessment approach used to determine the overall risk posture of a system, and addresses security concerns that may affect the system. A RAR is part of the security authorization package submitted to the Authorizing Official (AO) or Delegated Authorizing Official (DAO) for authorization of an NSS. This template follows guidance contained in NIST SP 800-30.

B. This Standard provides a template for preparing an RAR in support of the RMF process as it applies to DHS NSS. The preparer should adapt the format as needed. The preparer should determine what information is appropriate to include for compliance with applicable information security policies, based on the organization's security policy guidance. Where practicable, the template provides specific instructions for completing specific sections.

1. Information required for inclusion in the RAR can be either provided directly within a completed template, or through reference to another document containing that information.

2. This template assumes the execution of the risk assessment methodology described in NIST SP 800-30.

3. Information in this template highlighted in yellow and in italics and delineated by angular brackets “< >” is general template guidance that should be removed after the RAR is developed.

4. Information in this template highlighted in yellow and delineated by square brackets “[ ]” is a placeholder describing a component of information (either with text or appropriate corresponding numerical data) that should be supplied, and the square brackets should afterwards be removed.

5. Information other than that within square “[ ]” or angular “< >” brackets is suggested for inclusion as written in the RAR.

6. As the RAR is updated with information specific to the DHS NSS, it is developed for, the overall classification and portion markings should be updated appropriately to protect the document and the information it contains.

[Agency/Organization Name]

RISK ASSESSMENT REPORT

FOR

[SYSTEM NAME (ACRONYM)]

Version [#]

[Month year]

This page intentionally left blank.

REVISION CHANGE NOTICE

DHS SYSTEM/DOCUMENT CHANGE RECORDS

DHS CHANGE/REVIEW CONTROL LOG			
NAME OF CHANGE	DATE OF CHANGE	DATE OF REVIEW	AUTHORIZED BY

This page intentionally left blank.

PREFACE

<This template preface presents background material and rationale for the development of a Risk Assessment Report applicable to Department of Homeland Security (DHS) National Security Systems (NSS).>

<If desired, the RAR developed from this template may contain a Preface section. The following wording may be used as guidance for the RAR Preface.>

This Risk Assessment Report (RAR) was developed by [identify team or individual who developed the plan] under the direction of the [specify DHS NSS manager for whom the work was performed] for use on designated National Security Systems.

This RAR is based upon a review of the environment, documentation, DHS regulations/guidance, and interviews with the information system personnel conducted between dates. In addition to this plan, [specify other security documentation developed as part of the same task; e.g., a System Security Report (SSP), Security Assessment Report (SAR), and Plan of Action and Milestones (POA&M)] have been developed under this task.

This page intentionally left blank.

TABLE OF CONTENTS

PREFACE iii
1 RISK ASSESSMENT REPORT FOR [SYSTEM NAME] 1
1.1 Purpose 1
1.2 Process overview 1
1.3 System Description 2
1.4 Risk Assessment Report Team 2
2 RISK ASSESSMENT APPROACH 3
3 RISK ASSESSMENT PROCESS 4
3.1 Prepare for the Risk Assessment 4
3.2 Conduct the Risk Assessment 8
4 RISK ASSESSMENT RESULTS 13
4.1 Summary Statistics 13
4.2 Detailed Results 14

Table of Tables

Table 3-1. Identification of Adversarial Threat Sources 8
Table 3-2. Identification of Non-Adversarial Threat Sources 8
Table 3-3. Identification of Threat Events 9
Table 3-4. Identification of Vulnerabilities 9
Table 3-5. Assessment of Predisposing Conditions 9
Table 3-6. Assessment Scale – Likelihood of Threat Event Initiation (Adversary) 10
Table 3-7. Assessment Scale - Likelihood of Threat Event Initiation (Non-adversary) 10
Table 3-8. Assessment Scale - Likelihood of Threat Event Having Undesirable Consequences/Impact 10
Table 3-9. Assessment Scale - Overall Likelihood 10
Table 3-10. Impact Definition 11
Table 3-11. Identification of Adverse Impacts 12
Table 3-12. Assessment Scale – Level of Risk 12
Table 3-13. Assessment Scale - Level of Risk as a Combination of Likelihood 13
Table 4-1. Risk Categorization Results 13
Table 4-2. Column Descriptions for Adversarial Risk Table 14
Table 4-3. Risk Table for Risks Due to Adversaries 15
Table 4-4. Column Descriptions for Non-Adversarial Risk Table 15
Table 4-5. Risk Table for Risks Due to Non-Adversarial Threats 16

This page intentionally left blank.

1 RISK ASSESSMENT REPORT FOR [SYSTEM NAME]

1.1 PURPOSE

<Refer to NIST SP 800-30, Section 2.3.2, "Assessment Approaches," for additional information on risk assessment approaches (i.e., quantitative, semi-quantitative, and qualitative).>

The purpose of this Risk Assessment Report (RAR) is to identify and evaluate information security risks associated with operating the [System Name] ([System Acronym]). This RAR provides a structured [quantitative/semi-quantitative/qualitative] assessment of the system and its operational environment. It addresses impacts, threats, vulnerabilities, risks, and security measures (also referred to as safeguards, security controls, or countermeasures).

Risk assessments are developed or updated throughout the RMF. The risk assessment provides the Authorizing Official (AO) with an updated risk picture reflecting the actual (versus planned) state of affairs with regard to system implementation, security control effectiveness, and the operational environment.

Risk assessments are often not precise instruments of measurement and can only reflect the limitations of the specific assessment methodologies, tools, and techniques employed. An organization should incorporate as much information as practical on particular risks during the prioritization process to appropriately determine the values for risks (e.g., very low, low, moderate, high, very high).

1.2 PROCESS OVERVIEW

The risk assessment (RA) process is conducted in three stages, with each phase often involving several steps. The assessment stages are:

1. Prepare for the Risk Assessment
    - Identify Purpose, Scope, and Assumption
        - Identify Purpose of this Assessment
        - Identify Scope of this Assessment
        - Identify Assumptions Used in this Assessment
    - Identify Information Sources
    - Define (or Redefine) the Risk Model

2. Conduct Risk Assessment
    - Identify threats
    - Identify vulnerabilities and predisposing conditions
    - Determine likelihoods
    - Determine impacts
    - Determine risks and uncertainties
    - Communicate the Results

3. Maintain Risk Assessment (not covered in this Report)

1.3 SYSTEM DESCRIPTION[1]

System: [System Name]
System Location(s): [System Location(s)]
System Boundaries: [Specify System boundaries]
Mission: [Provide 1-2 paragraph executive overview of the mission(s) the system support]

The overall system security categorization is rated, in accordance with CNSSI 1253, as:

Security Objective	Security Categorization
Confidentiality	[Low/Moderate/High]
Integrity	[Low/Moderate/High]
Availability	[Low/Moderate/High]

1.4 RISK ASSESSMENT REPORT TEAM

This RAR was conducted by [identify Agency Office conducting the RAR] during [timeframe of the RA]. The Points of Contact for questions relating to this RAR are:

[Primary Point of Contact's name]
[Primary Point of Contact's job title/function]
[Primary Point of Contact's email(s)]
[Primary Point of Contact's telephone number(s)]

[Secondary Point of Contact's name]
[Secondary Point of Contact's job title/function]
[Secondary Point of Contact's email(s)]
[Secondary Point of Contact's telephone number(s)]

[1] For a more detailed system description, please refer to the NSS's System Security Plan (SSP).

2 RISK ASSESSMENT APPROACH

<Use and update this section as appropriate unless the risk assessment that is the subject of the report uses a different methodology.>

This risk assessment was completed using the methodology described in the National Institute of Standards and Technology Special Publication 800-30, *Guide to Conducting Risk Assessments* (dated September 18, 2012).

<The RAR Team should select the appropriate paragraph to include here depending upon the purpose of the RAR (i.e., initial and incomplete in support of Security Categorization, initial and completed based on security controls selection, updated to inform authorization, differential to inform risk response or how changes to a system may affect its risk posture, or incremental to determine whether there has been an system risk increase). The other paragraph should be removed prior to submission of the RAR.>

*<For an **initial** RA, select this paragraph for inclusion in the RAR.>*

This initial risk assessment for [System Name] identifies and evaluates the threats to and anticipated security vulnerabilities in the proposed system affecting confidentiality, integrity, and availability of the system in the context of the planned operational environment. It concludes with a comprehensive table providing a description of the threat, its characteristics, and associated threat level.

*<For a **reassessment** RA, select this paragraph for inclusion in the RAR.>*
This reassessment was conducted to assess the posture of [System Name] to update the Risk Assessment Report(s) (RAR) dated [insert date of previous RAR], as a result of [insert event that triggered reassessment]. This RAR includes an identification and description of the threats to and known vulnerabilities and predisposing conditions associated with the system an assessment of the risk posed by each. It also includes an assessment of the overall risk to the organization, and the data contained in the system, by operating the system evaluated.

3 RISK ASSESSMENT PROCESS

This section describes the risk assessment process performed during this effort. The process is divided into prepare, conduct, and maintain phases.[2]

<Depending on the objective of the risk assessment (i.e., which step in the Risk Management Framework (RMF) or focus within Tier 2 this risk assessment supports), certain elements in this risk assessment process and template will not be applicable. For those elements determined to be out of scope for this RMF step, an annotation should be made justifying their exclusion.>

3.1 PREPARE FOR THE RISK ASSESSMENT

<Refer to NIST SP 800-30, Section 3.1, "Preparing for the Risk Assessment" for additional information related to this stage.>

STEP 1: IDENTIFY PURPOSE, SCOPE, AND ASSUMPTIONS

<Refer to NIST SP 800-30, Section 3.1, Step 1, Tasks 1-1 to 1-3 for additional guidance related to this Step.>

Risk Assessment Purpose

<Describe the purpose of the risk assessment that is the subject of this report (why this is being done —initial, reassessment based on new risk identified, reassessment based on the need to determine best risk response option). The purpose should be stated clearly and in sufficient detail to ensure that the assessment produces the information and decisions it is intended to support. Usually, the purpose will be one of the two specified below.>

*<For an **initial** RA, select this paragraph for inclusion in the RAR.>*
This risk assessment provides an independent review to help [Agency or Organization Name] determine the appropriate level of security required for the system to support the development of a System Security Plan for [System Name]. It also provides guidance on security controls to address the risks identified in this assessment.

*<For a **reassessment** to the initial RA, select this paragraph for inclusion in the RAR.>*
This risk assessment provides an independent review and update to the risk assessment conducted on [insert date of prior RAR] to help the [Agency Name]'s Chief Information Security Officer (CISO) and Authorizing Official (AO) make an informed decision about [select one or more: continued authorization, reviewing risk response options for addressing select threats, or others] for [System Name].

Risk Assessment Scope

<Describe the scope of this risk assessment in terms of how the decisions it supports will be implemented and the boundaries of this assessment. Include what parts of the organization are involved or impacted and how. Identification of scope commonly includes the following elements (for all tiers unless otherwise specified). Example scope statements are provided for each area that should be addressed.>

[2] The maintain phase will not be covered by this RAR.

- This risk assessment will inform decisions for all systems supporting [specify mission/business function (Tier 2) or set of closely related functions (Tier 1)].

- This risk assessment will inform decisions to select, tailor, and/or supplement security controls for [specify system or set of common controls] (Tier 3) and to accept those controls as sufficient to meet the requirements of [specify mission/business function or segment] (Tier 2).

Organizational Applicability: *<Identify the parts of the organization that are affected by the risk assessment and the risk-based decisions resulting from the assessment.>*

- This risk assessment will affect [specify affected parts of the organization], specifically [describe how the parts of the organization are/will be affected].

Timeframe: *<Identify the timeframe where the decisions apply and/or the circumstances for revisiting decisions at a later time. >*

- This risk assessment is expected to remain valid as a source of decision support for [specify timeframe], unless [specify circumstances, which will be identified via risk monitoring and/or expressed in terms of milestones].

> *Note:* The determination of the timeframe is strongly related to the goals of the assessment. For example, a risk assessment to inform Tier 1 policy decisions needs to be relevant for a long time, since the governance process for policy changes tends to be time-consuming and onerous in most organizations. However, a risk assessment to inform a Tier 3 decision regarding the use of a compensating control, because a given control cannot be implemented in the current release of the system, should be relevant only until the next release.

Architectural scope: *<Determine the types of systems or operational environments where the decisions apply (Tiers 1 and 2).>*

- This risk assessment will inform decisions for all systems that operate in [specify environment (e.g., land-based fixed-facility)]. (Tier 1 or Tier 2 if all such systems are part of a single mission/business segment.)

Technical scope: *<Determine the types of technologies where the decisions apply (Tiers 1 and 2).>*

- This risk assessment will inform decisions for all systems that use or incorporate [specify technology (e.g., wireless communications, mobile code)]. (Tier 1 or Tier 2 if all such systems are part of a single mission/business segment.)

Risk Assessment Assumptions

<Describe the assumptions used in the risk assessment that is the subject of this report. Assumptions will commonly be provided in the form specified below.>

The assumptions used in this risk assessment based on organizational direction and assessment team expertise include the following [identify appropriate assumptions, using the relevant ones below]:

- This risk assessment assumes the effectiveness of common controls implemented by [Agency's name] in meeting specified requirements.
- This risk assessment assumes the correctness, completeness, and currency of risk assessments for the components of the mission/business segment.
- This risk assessment assumes the effectiveness of continuous monitoring for the components of the mission/business segment, and of risk monitoring (in particular, tracking of changes in the threat environment) at the organizational tier.
- This risk assessment assumes the following information-related, technical, operational, and environmental characteristics of [System, Network, Connection, Application, Contract for IT Services]: [specify, using NIST SP 800-30, Appendix D, Tables D-1 and D-2]. These characteristics affect the relevance of threats and security measures.
- This risk assessment will be reassessed [timeframe or circumstances for next update].

STEP 2: IDENTIFY INFORMATION SOURCES

<Refer to NIST SP 800-30, Section 3.1, Task 1-4, "Identify the sources of descriptive, threat, vulnerability, and impact information to be used in the risk assessment," for additional information and guidance related to this step and identifying sources of descriptive threat, vulnerability, and impact information to be used in the risk assessment.>

<Describe how data was collected. The following is a typical description/example; adjust by identifying sources of threat information, which should include the Enterprise Threat Statement. >

The data collection phase included identifying and interviewing key personnel within the organization and conducting document reviews. The interviews focus on the operating environment. The document reviews provided the risk assessment team with the basis on which to evaluate compliance with policy and procedure.

Additional data collection was conducted through the use of automated vulnerability scanners, manual inspection of the state of various controls (i.e., technical, process, operational, and management) and penetration testing (PenTest) as appropriate. Threat information was collected from sources [identify sources].

The following templates and worksheets were used by the risk assessment team and are included in the appendices:

<The following list contains examples of templates and worksheets that are recommended for use in a risk assessment. Replace with the names of the templates and worksheets actually used.>

- [**NIST SP 800-53, Revision 3, Security Baseline Worksheet:** Completed by the analysts using information extracted from questionnaires and interviews.]
- **[Risk Calculation Worksheet:** Converts the raw vulnerabilities into risks based on the following methodology:]
  - [Categorizing vulnerabilities]

  - [Pairing with threat vectors]
  - [Assessing the probability of occurrence (likelihood) and possible impact]
- **[Risk Mitigation Worksheet:** Lists the risks and the associated recommended controls to mitigate these risks for review.]

The following describes the information sources used in this assessment:
<Refer to NIST SP 800-30, Section 3.1, Task 1-4 Task 1-4, "Identify the sources of descriptive, threat, vulnerability, and impact information to be used in the risk assessment.">

- Threat sources: [Identify which threat sources were used in this assessment using NIST SP 800-30, Appendix D.]
- Threat events: [Identify the source of threat events used in this assessment. What set of threat events served as the starting point for the identification of threat events in this risk assessment?]

  Note: NIST SP 800-30, Appendix E, Tables E-1 "Inputs – Threat Event Identification," E-2, "Representative Examples – Adversarial Threat Events," E-3, "Representative Examples – Non-Adversarial Threat Events," and E-4, "Relevance of Threat Events," provide guidance for DHS to eliminate, modify, or predict certain threat events and the relevance of those threat events as a starting point for the risk assessment.

- Vulnerabilities and predisposing conditions: [Identify specific techniques used to identify vulnerabilities and predisposing conditions as part of an initial risk assessment report during RMF Task 1-2 and update the risk assessment report as needed throughout the RMF.] *<For additional guidance, refer to NIST SP 800-30, Appendix F.>*

  Note: Vulnerabilities may be described using a dictionary of common names from publicly known information system vulnerabilities sources, such as the Common Vulnerabilities and Exposures (CVE) enumeration.[3]

- Impact: [Identify how the potential impact level was assessed. What types of consequences were considered?]

  Note: Impact levels, as defined in CNSSI 1253, provide a starting point for assessing potential impact levels.

- Risk tolerance: [Identify levels and types of risk as well as degree of risk uncertainty that were considered acceptable as identified by the Risk Executive Function. What levels of risk, or of likelihood and/or impact, were used to decide that no further analysis (of risk response alternatives, or of threat events) would be conducted (if any)?]

STEP 3: DEFINE (OR REFINE) THE RISK MODEL

<Refer to NIST SP 800-30, Section 3.1, Task 1-5, "Identify the risk model and analytic approach to be used in the risk assessment," for additional information and guidance related to this step.>

<Define (or Redefine) the risk model used for this RAR using NIST SP 800-30, Section 2.3.2.>

[3] As cited in CNSSI 4009.

This RAR uses a [quantitative/qualitative/semi-quantitative] assessment approach(es) to conduct the risk assessment. [Include a description of the approach, an example for each approach as appropriate, and an organizational and a mission/business function example (if possible). If using a semi-quantitative approach, be sure to include "break points" between bins as rationale for how values were distributed; also include additional examples for the "middle" bin since this bin should cover a wider range than the two extremes.]

3.2 CONDUCT THE RISK ASSESSMENT

<Refer to NIST SP 800-30 Chapter 3, Section 3.2.for additional information related to this stage.>

STEP 1: IDENTIFY THREAT SOURCES

<Refer to NIST SP 800-30, Section 3.2, Task 2-1,"Identify Threat Sources" and Appendix D for additional information related to this stage.>

<List applicable threats per adversary type and threat source per Tables 3-1 (refer to NIST SP 800-30, Appendix D, Table D-7) and 3-2 (refer to NIST SP 800-30, Appendix D, Table D-8) below. The below Identifiers in Table 3-1 and Table 3-2 are not to be considered all-inclusive and should be updated with organizationally-defined identifiers, using NIST SP 800-30, Appendix D, Table D-2 as guidance.>

Potential threats to [System Name] and used in this assessment were identified and characterized through the following:

Table 3-1. Identification of Adversarial Threat Sources

Identifier	Threat Source Source of Information	In-Scope? (Yes/No)	Capability	Intent	Targeting
1.A.i Individual Outsider					
1.A.ii Insider					
1.A.iii Trusted Insider					
1.A.iv Privileged Insider					
1.B.i Ad-hoc Group					
1.B.ii Established Group					
1.C Organization					
1.D Nation-state					

Table 3-2. Identification of Non-Adversarial Threat Sources

Identifier	Threat Source Source of Information	In-Scope?	Range of Effects
2.A Error by Ordinary User			
2.B Error by Privileged User / Administrator			
3.A Failure of IT Equipment			
3.B Failure of Environmental Controls			
4.A Natural or man-made disaster			
4.B Unusual natural event			
4.C Infrastructure failure / outage			

The identified threat events and the suspected sources of threat events (or causal agents) to [System Name] were identified and characterized from the following sources: *< List applicable*

threat events per identifier in Table 3-3 (refer to NIST SP 800-30, Appendix E).>

Table 3-3. Identification of Threat Events

Identifier	Threat Event Source of Information	Threat Source	Relevance
[Threat Event]			
[Threat Event]			
[Threat Event]			

Output: Results from this step were used as input for Table 4.3, "Risk Table for Risks Due to Adversaries" (below), and Table 4.5, "Risk Table for Risks Due to Non-Adversarial Threats" (below).

STEP 2: IDENTIFY VULNERABILITIES AND PREDISPOSING CONDITIONS

<Refer to NIST SP 800-30, Section 3.2, Task 2-3, "Identify Vulnerabilities and Predisposing Conditions," and Appendix F.>

<Update the following introduction to this section as appropriate to the system undergoing the risk assessment and the processes used.>

The identification of vulnerabilities and characteristics of [System Name] and its [mission/business segment, or of the system, or set of common controls in its operational environment], which affect the likelihood that a threat event will result in undesirable consequences were assessed.

Output: Results from this step identified the vulnerabilities in Table 3-4, "Identification of Vulnerabilities" (below), predisposing conditions and extent of the condition in the environment in Table 3-5, "Assessment of Predisposing Conditions" (below).

< List applicable threat events per identifier in Table 3-4 (refer to NIST SP 800-30, Appendix F, Table F-3) and Table 3-5 (refer to NIST SP 800-30, Appendix F).>

Table 3-4. Identification of Vulnerabilities

1	2	3
Identifier	Vulnerability Source of Information	Vulnerability Severity
	[Vulnerability]	
	[Vulnerability]	

Table 3-5. Assessment of Predisposing Conditions

1	2	3
Identifier	Predisposing Condition Source of Information	Pervasiveness of Condition
	[Predisposing Condition]	
	[Predisposing Condition]	

STEP 3: DETERMINE LIKELIHOOD

<Refer to NIST SP 800-30, Section 3.2, Task 2-4, "Determine Likelihood," and Appendix G for additional information and guidance related to this step.>

The likelihood of adverse events occurring and resulting in undesirable consequences was

determined by taking into consideration each identified threat source and threat event (as identified in Table 3-1, Table 3-2, and Table 3-3 above), vulnerabilities and predisposing conditions (as identified in Table 3-4 and Table 3-5 above), as well as the susceptibility of mission/business functions to adverse events as identified in mission/business analyses and/or as derived from documentation of mission/business threads and/or the segment architecture. The scales of likelihood provided in tables (below) were used in this determination.

Table 3-6. Assessment Scale – Likelihood of Threat Event Initiation (Adversary)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Adversary is almost certain to initiate the threat event.
High	80-95	8	Adversary is highly likely to initiate the threat event.
Moderate	21-79	5	Adversary is somewhat likely to initiate the treat event.
Low	5-20	2	Adversary is unlikely to initiate the threat event.
Very Low	0-4	0	Adversary is highly unlikely to initiate the threat event.

Table 3-7. Assessment Scale - Likelihood of Threat Event Initiation (Non-adversary)

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year.
High	80-95	8	Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year.
Moderate	21-79	5	Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year.
Low	5-20	2	Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.
Very Low	0-4	0	Error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years.

Table 3-8. Assessment Scale - Likelihood of Threat Event Having Undesirable Consequences/Impact

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	If the threat event is initiated or occurs, it is almost certain to have undesirable consequences or adverse impacts.
High	80-95	8	If the threat event is initiated or occurs, it is highly likely to have undesirable consequences or adverse impacts.
Moderate	21-79	5	If the threat event is initiated or occurs, it is somewhat likely to have undesirable consequences or adverse impacts.
Low	5-20	2	If the threat event is initiated or occurs, it is unlikely to have undesirable consequences or adverse impacts.
Very Low	0-4	0	If the threat event is initiated or occurs, it is highly unlikely to have undesirable consequences or adverse impacts.

Table 3-9. Assessment Scale - Overall Likelihood

Likelihood of Threat Event	Likelihood Threat Events Result in Undesirable Consequences or Adverse Impacts

Initiation or Occurrence	Very High	High	Moderate	Low	Very Low
Very High	Very High	Very High	High	Moderate	Low
High	Very High	High	High	Moderate	Low
Moderate	High	Moderate	Moderate	Low	Low
Low	Moderate	Low	Low	Low	Low
Very Low	Low	Low	Very Low	Very Low	Very Low

Output: The results generated in this step were used to update Table 4-3, "Risk Table for Risks Due to Adversaries" (below), and Table 4-5, "Risk Table for Risks Due to Non-Adversarial Threats" (below).

STEP 4: DETERMINE IMPACT

<Refer to NIST SP 800-30, Section 3.2, Task 2-5,"Determine Impact," and Appendix H for additional information and guidance related to this step.>

The impact of each identified threat (from Table 3-1 and Table 3-2 [above]) that could result in undesirable consequences was assessed, as were the impacts of identified threat events (from Table 3-3 [above]). The definitions of impact provided in Table 3-10 (below) were used in this assessment. The results are provided in Table 3- 11 (below).

Table 3-10. Impact Definition

Qualitative Values	Semi-Quantitative Values		Description
Very High	95-100	10	The event could have **multiple severe or catastrophic adverse effects** on organizational operations, organizational assets, individuals, other organizations, and/or the national security interests of the United States.
High	85-94	8	The event could have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States. A severe or catastrophic adverse effect means that the event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions for a significant period of time; (ii) severely undermine the ability to perform one or more of the primary functions for a significant period of time; (iii) result in major damage to organizational, critical infrastructure, or national security assets; (iv) result in major financial loss; or (v) result in severe or catastrophic harm to individuals exceeding mission expectations.
Medium	25-84	5	The event could have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States. A serious adverse effect means that the event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is significantly reduced; (ii) result in significant damage to organizational, critical infrastructure, or national security assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals exceeding mission expectations.
Low	5-24	2	The event could have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States. A limited adverse effect means that the event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of those functions is noticeably reduced; (ii) result in minor damage to organizational, critical infrastructure, or national security assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Qualitative Values	Semi-Quantitative Values		Description
Very Low	0-4	0	The event could have a minor adverse effect on organizational operations, organizational assets, individuals, or other organizations. A minor adverse effect means that the event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary and secondary functions, but the effectiveness of some of those functions is noticeably reduced; (ii) result in minor damage to organizational, critical infrastructure; or (iii) result in minor financial loss.

Table 3-11. Identification of Adverse Impacts

1	2	3	4
Type of Impact	Impact Affected Asset	Security Objectives Not Achieved	Maximum Impact

Output: Results from this step were used to update Table 4-3, "Risk Table for Risks Due to Adversaries" (below), and Table 4-5, "Risk Table for Risks Due to Non-Adversarial Threats" (below).

STEP 5: DETERMINE RISKS AND UNCERTAINTIES

<Refer to NIST SP 800-30, Section 3.2, Task 2-6, "Determine Risk," and Appendix I for additional information and guidance related to this step.>

In this step, the risk assessment team compiled the results of each of the preceding four steps and determined the degree of risk to the system from each identified vulnerability.

Risk Determination: Table 3-12 (below) provides a definition for the risk levels used in this assessment**.** These levels represent the assessed degree or level of risk to which an organization, IT system, or facility would be exposed if a given vulnerability were exploited.

Table 3-12. Assessment Scale – Level of Risk

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	**Very high risk** means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	21-79	5	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	5-20	2	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	0-4	0	**Very low risk** means that a threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Table 3-13 (below) defines a function by which likelihood and impact are combined to determine the risk level. If any one threat, vulnerability, likelihood or impact is determined to be zero,

there is no risk.

Table 3-13. Assessment Scale - Level of Risk as a Combination of Likelihood and Impact Level

Likelihood that Threat Event Will Occur and Result in Undesirable Consequences	Impact Level				
	Very Low	Low	Medium	High	Very High
Very High	Low	Medium	High	Very High	Extremely High
High	Low	Medium	Medium	High	Very High
Medium	Very Low	Low	Medium	Medium	High
Low	Very Low	Low	Low	Low	Medium
Very Low	Very Low	Very Low	Very Low	Low	Low

Output: The results of this step were used to complete Table 4-2, "Risk Table for Risks Due to Adversaries" (below), and Table 4-5, "Risk Table for Risks Due to Non-Adversarial Threats" (below).

4 RISK ASSESSMENT RESULTS

4.1 SUMMARY STATISTICS

Summary statistics for the potential risks identified in this assessment for [System Name] are presented in Table 4-1 and Figure 4-1. Table 4-1 identifies the risk categorization results for the risks identified in this assessment based on the assessed values for likelihood and level of impact. Figure 4-1 depicts the sum of risks identified at each risk level and their relative proportions.

<Update Table 4-1 with the information derived from the risk assessment. Populate Table 1-1 with the same information so that Table 1-1 and Table 4-1 contain identical information.>

Table 4-1. Risk Categorization Results

Likelihood that Threat Event Will Occur and Result in Undesirable Consequences	Level of Impact				
	Very Low	Low	Medium	High	Very High
Very High	3	3	5	5	3
High	2	1	4	4	5
Medium	1	5	2	4	9
Low	3	4	5	6	2
Very Low	2	7	6	9	4

<Create Figure 4-1 using the results from the risk assessment (as indicated in Table 4-1). Copy Figure 4-1 to create Figure 1-1 so that they both contain identical Information. This type of chart can be created using MS Excel and imported into this document.>

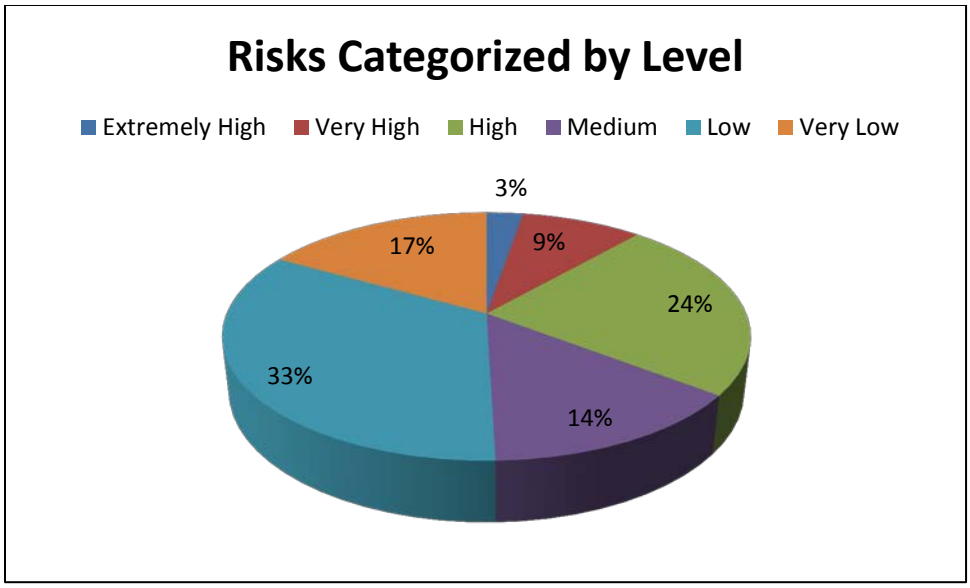

Figure 4-1 - Risks Categorized by Level

4.2 DETAILED RESULTS

Detailed results for the potential risks identified in this assessment for [System Name] are presented in and Table 4-5. Table 4-2 and Table 4-4 describe the identified risks (due to adversaries and non-adversarial threats, respectively), including their assessed likelihood and impact. Table 4-2 describes the contents of each of the columns of, and Table 4-4 describes the contents of each of the columns of Table 4-5.

Table 4-2. Column Descriptions for Adversarial Risk Table

Column	Heading	Content
1	Threat Event	Identify threat event. (NIST SP 800-30 Task 2-2, Ta ble E-1, Table E-2, Table E-5, Table I-5)
2	Threat Sources	Identify threat sources that could initiate the threat event. (NIST SP 800-30 Task 2-1, Table D-1, Table D-2, Table D-7, Table I-5)
3	Capability	Assess threat source capability. (NIST SP 800-30 Task 2-1, Table D-3, Table D-7, Table I-5)
4	Intent	Assess threat source intent. (NIST SP 800-30 Task 2-1, Table D-4, Table D-7, Table I-5)
5	Targeting	Assess threat source targeting. (NIST SP 800-30 Task 2-1, Table D-5, Table D-7, Table I-5)
6	Relevance	Determine relevance of threat event. (NIST SP 800-30 Task 2-2, Table E-1, Table E-4, Table E-5, Table I-5) If the relevance of the threat event does not meet the organization's criteria for further consideration, do not complete the remaining columns.
7	Likelihood of Attack Initiation	Determine likelihood that one or more of the threat sources initiates the threat event, taking into consideration capability, intent, and targeting. (NIST SP 800-30 Task 2-4, Table G-1, Table G-2, Table I-5)
8	Vulnerabilities and Predisposing Conditions	Identify vulnerabilities which could be exploited by threat sources initiating the threat event, the predisposing conditions which could increase the likelihood of undesirable consequences and/or adverse impacts. (NIST SP 800-30 Task 2-5, Table F-1, Table F-3, Table F-4, Table F-6, Table I-5)
9	Severity and Pervasiveness	Assess severity of vulnerabilities and pervasiveness of predisposing conditions. (NIST SP 800-30 Task 2-5, Table F-1, Table F-2, Table F-5, Table F-6, Table I-5)
10	Likelihood that Initiated Attack Succeeds	Determine the likelihood that the threat event, once initiated, will result in undesirable consequences, taking into consideration threat source capability, vulnerabilities, and

		predisposing conditions. (NIST SP 800-30 Task 2-4, Table G-1, Table G-4, Table I-5)
11	Overall Likelihood	Determine the likelihood that the threat event will be initiated and result in undesirable consequences (i.e., combination of likelihood of attack initiation and likelihood that initiated attack succeeds). (NIST SP 800-30 Task 2-4, Table G-1, Table G-5, Table I-5)
12	Undesirable Consequences Affected Assets	Determine the undesirable consequences (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) of the threat event.
13	Level of Impact	Determine the level of impact associated with the undesirable consequences of the threat event. (NIST SP 800-30 Task 2-5, Table H-1, Table H-2, Table H-3, Table H-4, Table I-5)
14	Risk	Determine the level of risk as a combination of likelihood and impact. (NIST SP 800-30 Task 2-6, Table I-1, Table I-2, Table I-3, Table I-5)

Table 4-3. Risk Table for Risks Due to Adversaries

1	2	3	4	5	6	7	8	9	10	11	12	13	14
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Characteristics	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Consequences / Affected Assets	Level of Impact	Risk
		Capability	Intent	Targeting									

Table 4-4. Column Descriptions for Non-Adversarial Risk Table

Column	Heading	Content
1	Threat Event	Identify threat event. (NIST SP 800-30 Task 2-2, Table E-1, Table E-3, Table E-5, Table I-7)
2	Threat Sources	Identify threat sources that could initiate the threat event. (NIST SP 800-30 Task 2-1, Table D-1, Table D-2, Table D-8, Table I-7)
3	Range of Effects	Identify the range of effects from the threat source (NIST SP 800-30 Task 2-1, Table D-1, Table D-6, Table I-7)
4	Relevance	Determine relevance of threat event. (NIST SP 800-30 Task 2-2, Table E-1, Table E-4, Table E-5, Table I-7) If the relevance of the threat event does not meet the organization's criteria for further consideration, do not complete the remaining columns.
5	Likelihood of Threat Event Occurring	Determine the likelihood that the threat event will occur. (NIST SP 800-30 Task 2-4, Table G-1, Table G-3, Table I-7)
6	Vulnerabilities and Predisposing Conditions	Identify vulnerabilities which could be exploited by threat sources initiating the threat event, and the predisposing conditions which could increase the likelihood of adverse impacts. (NIST SP 800-30 Task 2-5, Table F-1, Table F-3, Table F-4, Table F-6, Table I-7)
7	Severity and Pervasiveness	Assess severity of vulnerabilities and pervasiveness of predisposing conditions. (NIST SP 800-30 Task 2-5, Table F-1, Table F-2, Table F-5, Table F-6, Table I-7)
8	Likelihood Threat Event Results in Adverse Impact	Determine the likelihood that the threat event, once initiated, will result in adverse impact, taking into consideration vulnerabilities and predisposing conditions. (NIST SP 800-30 Task 2-4, Table G-1, Table G-4, Table I-7)
9	Overall Likelihood	Determine the likelihood that the threat event will occur and result in adverse impacts (i.e., combination of likelihood of threat occurring and likelihood that the threat event results in adverse impact). (NIST SP 800-30 Task 2-4, Table G-1, Table G-5, Table I-7)
10	Consequences/	Determine the consequences (i.e., potential harm to organizational operations, organizational

	Affected Assets	assets, individuals, other organizations, or the Nation) of the threat event.
11	Level of Impact	Determine the adverse impact (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) from the threat event. (NIST SP 800-30 Task 2-5, Table H-1, Table H-2, Table H-3, Table I-7)
12	Risk	Determine the level of risk as a combination of likelihood and impact. (NIST SP 800-30 Task 2-6, Table I-1, Table I-3, Table I-7)

Table 4-5. Risk Table for Risks Due to Non-Adversarial Threats

1	2	3	4	5	6	7	8	9	10	11	12
Threat Event	Threat Sources	Range of Effects	Relevance	Likelihood of Event Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Event Results in Adverse Impact	Overall Likelihood	Consequences / Affected Assets	Level of Impact	Risk