APPENDIX C: RISK ASSESSMENT REPORT TEMPLATE

RISK ASSESSMENT REPORT (RAR)

<ORGANIZATION>
<SYSTEM NAME>
<DATE>

Record of Changes:

Version	Date	Sections Modified	Description of Changes
1.0	DD MM YY	Initial RAR	

System Description

The <*System Name/Unique Identifier*> consists of <*System Description*> processing <*Classification Level*> data. The risk categorization for this system is assessed as <*e.g., Moderate-Low-Low*>.

< System Name/Unique Identifier> is located *<insert physical environment details>.* The system *<list all system connections and inter-connections, or state "has no connections, (wired or wireless)>.* This system is used for *<system purpose/function>,* in support of performance on the *<list all program and/or contract information>*. The system *<provide any system-specific details, such as Mobility>*.

The Information Owner is *<insert POC information, including address and phone number>.*

The Information System Security Manager (ISSM) is *<insert Point of Contact (POC) information, including address and phone number>.*

The Information System Security Officer (ISSO) is *<insert POC information, including address and phone number>.*

Scope

The scope of this risk assessment is focused on the system's use of resources and controls to mitigate vulnerabilities exploitable by threat agents (internal and external) identified during the Risk Management Framework (RMF) control selection process, based on the system's categorization.

This initial assessment will be a Tier 3 or "information system level" risk assessment. While not entirely comprehensive of all threats and vulnerabilities to the system, this assessment will include any known risks related to the incomplete or inadequate implementation of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 controls selected for this system. This document will be updated after certification testing to include any vulnerabilities or observations by the independent

assessment team. Data collected during this assessment may be used to support higher level risk assessments at the mission/business or organization level.

<Identify assumptions, constraints, timeframe. This section will include the following information:

- *Range or scope of threats considered in the assessment*
- *Summary of tools/methods used to ensure NIST SP 800-53 compliance*
- *Details regarding any instances of non-compliance*
- *Relevant operating conditions and physical security conditions*
- *Timeframe supported by the assessment (Example: security-relevant changes that are anticipated before the authorization, expiration of the existing authorization, etc.).>*

Purpose

<Provide details on why this risk assessment is being conducted, including whether it is an initial or other subsequent assessment, and state the circumstances that prompted the assessment. Example: This initial risk assessment was conducted to document areas where the selection and implementation of RMF controls may have left residual risk. This will provide security control assessors and authorizing officials an upfront risk profile.>

Risk Assessment Approach

This initial risk assessment was conducted using the guidelines outlined in the NIST SP 800-30*, Guide for Conducting Risk Assessments*. A *<SELECT QUALITATIVE / QUANTITATIVE / SEMI-QUANTITATIVE>* approach will be utilized for this assessment. Risk will be determined based on a threat event, the likelihood of that threat event occurring, known system vulnerabilities, mitigating factors, and consequences/impact to mission.

The following table is provided as a list of sample threat sources. Use this table to determine relevant threats to the system.

Table 1: Sample Threat Sources (see NIST SP 800-30 for complete list)

TYPE OF THREAT SOURCE	DESCRIPTION
ADVERSARIAL - Individual (outsider, insider, trusted, privileged) - Group (ad-hoc or established) - Organization (competitor, supplier, partner, customer) - Nation state	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (e.g., information in electronic form, information and communications, and the communications and information-handling capabilities provided by those technologies.)

TYPE OF THREAT SOURCE	DESCRIPTION
ADVERSARIAL - Standard user - Privileged user/Administrator	Erroneous actions taken by individuals in the course of executing everyday responsibilities.
STRUCTURAL - IT Equipment (storage, processing, comm., display, sensor, controller) - Environmental conditions • Temperature/humidity controls • Power supply - Software • Operating system • Networking • General-purpose application • Mission-specific application	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.
ENVIRONMENTAL - Natural or man-made (fire, flood, earthquake, etc.) - Unusual natural event (e.g., sunspots) - Infrastructure failure/outage (electrical, telecomm)	Natural disasters and failures of critical infrastructures on which the organization depends, but is outside the control of the organization. Can be characterized in terms of severity and duration.

The following tables from the NIST SP 800-30 were used to assign values to likelihood, impact, and risk:

Table 2: Assessment Scale – Likelihood of Threat Event Initiation (Adversarial)

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 threat 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: Assessment Scale – Likelihood of Threat Event Occurrence (Non-adversarial)

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 per year**.
High	80-95	8	Error, accident, or act of nature is **highly likely** to occur; or occurs **between 10-100 times per year**.
Moderate	21-79	5	Error, accident, or act of nature is **somewhat likely** to occur; or occurs **between 1-10 times per 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 4: Assessment Scale – Impact of Threat Events

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The 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	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat 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; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Qualitative Values	Semi-Quantitative Values		Description
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat 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 the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat 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 the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Table 5: Assessment Scale – Level of Risk

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	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	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	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	Threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Qualitative Values	Semi-Quantitative Values		Description
Very Low	0-4	0	Threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.

Table 6: Assessment Scale – Level of Risk (Combination of Likelihood and Impact)

Likelihood (That Occurrence Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Risk Assessment Approach

Determine relevant threats to the system. List the risks to system in the Risk Assessment Results table below and detail the relevant mitigating factors and controls. Refer to NIST SP 800-30 for further guidance, examples, and suggestions.

Risk Assessment Results

Threat Event	Vulnerabilities / Predisposing Characteristics	Mitigating Factors	Security Control(s)	Likelihood (Tables 2 & 3)	Impact (Table 4)	Risk (Tables 5 & 6)
e.g. Hurricane	*Power Outage*	*Backup generators*	*PE-12*	*Moderate*	*Low*	*Low*

* Likelihood / Impact / Risk = Very High, High, Moderate, Low, or Very Low

_____

Signature
Government Information Owner

_____

Printed Name, Title, and Phone Number

Note: *Information Owner acknowledgment is only provided if necessary or required by the DCSA AO. (Examples: Legacy Operating Systems, Risk concerns raised based on the results of the RAR, deviations from the DCSA baseline, etc.)*