

**ADVANCED SYSTEMS & TECHNOLOGY**

**(U) ATTACHMENT J-9, OPEN FRAMEWORK INFORMATION SECURITY SELF-ASSESSMENT**

**(U) Version 2.0, 5 November 2021**

***(U) Part of AS&T’s FY21-22 Open BAA Framework – Architecture After Next***

**(U) CHANGE MANAGEMENT LOG**

**for**

**ATTACHMENT J-9, OPEN FRAMEWORK ISSA**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **VERSION** | **DATE** | **REVISED BY** | **AREA AFFECTED** | **REMARKS** |
| 1.0 | 15 October 2020 | Karen McGrath | All | Initial Release. |
| 2.0 | 17 November 2021 | Jennifer A. Hughes | Section 3 | Removed Section 3, References and renumbered accordingly |
| Section 5.2 | Renumbered Section 5.1. |
| Section 5.3 | Renumbered Section 5.2. |
| New Section 5.2, Item g | Modified as indicated in red. |
| Section 5.4, Item n | Added. |
| Section 5.5 | Added. |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| **NOTE**: Process for all Framework document version control: Initial version will be 1.0. Identify subsequent versions in the same FY by numerically increasing the number following the decimal, e.g., 1.**1**, 1.**2**, 1.**3**, etc. When an update in the following FY is required, the numerical version will change from **1**.X, to **2**.X, etc. If no changes are required in a given FY, a numerical change is not required. The review of all Framework documents occurs at FY-end and documented in requisite CMLs per guidance herein. | | | | |
| **Table is Unclassified** | | | | |

**(U) Information Security Self-Assessment Form**

**(U) created directly from Version 5.1, 19 July 2021**

# (U) Purpose

There are categories of unclassified information that require protective measures to restrict and control distribution for a variety of reasons. These categories of controlled unclassified information include Sensitive but Unclassified information (SBU), proprietary information (PROPIN) related to National Reconnaissance Office (NRO) activities, Controlled Unclassified Information (CUI), and For Official Use Only (FOUO) information. These types of sensitive information for NRO programs and activities are marked with dissemination controls such as “SBU,” “PROPIN,” “CUI,” or “FOUO.” When handling, processing, or storing these types of information on non-government, non-NRO information systems, all persons shall comply with this NRO Directive (ND) 100-37, “Security of Controlled Unclassified NRO Information on Non-Government, Non-NRO Information Systems.”

Protection of this type of sensitive information will be assessed by a review of this completed Information Security Self-Assessment (ISSA). The ISSA is based on the requirements contained in ND 100-37; ND 100-2 “FOUO Information Handling”; NRO Information Assurance Standards Document (IASD) Rev. C; and, NIST Special Publication 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

# (U) Instructions

* Offeror’s that will utilize an UNCLASSIFIED information system / network for any portion of this effort shall complete the entire ISSA (sections 3.0 – 5.0) with the exception of section 6.0.
* Offeror’s that will utilize an existing CLASSIFIED information system / network for any portion of this effort shall complete sections 3.0, 4.0, and 6.0.
* Government Sources Sought Announcement (GSSA) projects must submit a written certification from the Information Systems Security Manager (ISSM) stating that all information systems / networks used on this project meet the minimum security requirements and standards. GSSA’s are open to U.S. Federal Government organizations and Federally Funded Research and Development Centers (FFRDCs) that are funded via Military Interdepartmental Purchase Requests (MIPRs). GSSA Offeror’s do not need to complete the ISSA.
  + The Aerospace Corporation and the MITRE Corporation are not eligible to participate due to their close, ongoing relationship with the NRO.
* University and college Offeror’s are exempt and do not need to complete the ISSA.

# ~~(U) References~~

* ~~(U) NRO Directive 100-37, Security of Controlled Unclassified NRO Information on Non-Government, Non-NRO Information Systems~~
* ~~(U) NRO Directive 100-2 FOUO Information Handling~~
* ~~(U) NRO Information Assurance Standards Document (IASD) Rev. C~~
* ~~(U) NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations~~

# (U) GENERAL INFORMATION

*Date*: \_\_\_\_\_\_\_\_\_\_\_

*3.1 (U) Offeror (Company or Individual) Name:*

*3.2 (U) Project/Contract Title:*

*3.3 (U) Project Site Location:*

*3.4 (U) Project Contacts:*

|  |  |  |  |
| --- | --- | --- | --- |
| **Contact** | **Name** | **Phone** | **Email** |
| Program Manager |  |  |  |
| Program Security |  |  |  |
| Physical Security |  |  |  |
| IT Security |  |  |  |
| System Administration |  |  |  |
| *Table is Unclassified*  *Upon filling table, classify appropriately* | | | |

# (u) PROGRAM SECURITY INFORMATION

*4.1 Project Security Classification Level (Select all that apply):*

UNCLASSIFIED  CONFIDENTIAL  SECRET  TOP SECRET  SCI  NOFORN

*4.2 UNCLASSIFIED Facility Description:*

Contractor/Industry Site  University/College  U.S. Government Site

*4.3 Will the project collect or store Personally Identifiable Information (PII)\*?*

☐ Yes  No

\*PII is any information about a person that can be used to identify the person such as a social security number, date of birth, address, passport information, financial records, health records, and criminal records.

# UNCLASSIFIED INFORMATION SYSTEM INFORMATION

*5.1 (U) UNCLASSIFIED Information System Users (select all that apply)*

|  |  |
| --- | --- |
| General Users: | U.S. Citizens  Permanent Resident Aliens  Foreign Nationals |
| Privileged Users\*: | U.S. Citizens  Permanent Resident Aliens  Foreign Nationals |
| **Table is Unclassified** | |

\* A privileged user is any user who is delegated elevated levels of access control to a system or network. Examples of PUs are system administrators, network administrators, root users, and super users.

*~~5.2 (U) Insert below or attach an unclassified System/Network Diagram~~*

**~~—INSERT UNCLASSIFIED SYSTEM/NETWORK DIAGRAM HERE—~~**

*5.2 (U) UNCLASSIFIED Information System Description*

|  |  |  |
| --- | --- | --- |
| **a)** Does the network have Internet access? | | Yes  No |
| **b)** Is the network in a demilitarized zone (DMZ), meaning a sub-network? | | Yes  No |
| **c)** Does the network use a firewall? | | Yes  No |
| **d)** Does the network use physical port security inside the perimeter? | | Yes  No |
| **e)** Are there any physical or logical connections to other organizational networks belonging to other companies, vendors, or business partners? | | Yes  No |
| *If “Yes” Describe Connection Type and List Purpose:* |  | |
| **f)** Does the network use Remote Access Services such as virtual private network (VPN)? | | Yes  No |
| *If “Yes” List VPN Software/Hardware Vendor and Type:* |  | |
| **g)** Are there any wireless connections ~~such as Wi-Fi~~? | | Yes  No |
| *If “Yes” Describe Security Measures for Wireless Connections:* |  | |
| **h)** Are there any mobile devices such as laptops, tablets, or smart phones connected to the network? | | Yes  No |
| *If “Yes” Describe Security Measures for Mobile Devices:* |  | |
| *If “Yes” List CDS Vendor and Describe:* |  | |
| **i)** Does the network utilize a storage area network (SAN) or network attached storage (NAS)? | | Yes  No |
| *If “Yes” List Storage Vendor/Solution Type, and Describe:* |  | |
|  |  | |
|  |  | |
| **j)** Does the network implement whole disk encryption? | | Yes  No |
| **k)** Does the network implement file-level encryption? | | Yes  No |
| **l)** Does the network utilize public key encryption such as PKI certificates? | | Yes  No |
| *If “Yes” List Public Key Encryption Vendor/Solution Type, and Describe:* |  | |
| **m)** Does the network use a 3rd party offsite cloud computing service or cloud storage solution (e.g. Dropbox, Google, Amazon, GoDaddy)? | | Yes  No |
| *If “Yes” List Cloud Vendor/Solution, Security Measures, and Purpose of Use:* |  | |
| **Table is Unclassified** | | |

*5.3 (U) Unclassified System / Network Diagram:*

*(U) Insert below or attach and submit with this document data flows, technical architecture / engineering diagrams, system boundary drawings.*

*5.4 (U) Unclassified Information System Protection of Sensitive Information: Describe the procedures on how each of the following security controls is implemented on the unclassified system. Responses should be sufficiently detailed and should* ***NOT be “Yes/No” answers****.*

|  |  |
| --- | --- |
| **Basic CUI Protection Requirement** | **Offeror Response** |
| **a.)** Prevent/prohibit controlled information from being processed or stored on publicly available information systems or personal portable electronic devices (unmanaged/non-organizationally owned). |  |
| **b.)** Cloud storage solutions must be secured to prevent unauthorized access and be approved by the NRO. |  |
| **c.)** Protect controlled information by at least one physical or electronic/logical barrier when not under the direct control of an authorized user. |  |
| **d.)** Remove controlled information from the system when no longer needed IAW NI 56-1-3, *Records Disposition and Preservation*. |  |
|  |  |
|  |  |
| **e.)** All FOUO information must be sufficiently marked. |  |
| **f.)** Encrypt all controlled information when stored on mobile devices (e.g., laptops, removable media) |  |
| **g.)** Limit the transfer of controlled information to subcontractor or teaming partners with need-to-know. |  |
| **h.)** Protect the confidentiality of controlled information in transit (e.g., encrypted email, TLS, VPN, closed networks, DoD SAFE). |  |
| **i.)** Encrypt and control access to wireless networks processing or storing controlled information. |  |
| **j.)** Utilize malware protection which is regularly updated (at least monthly). |  |
| **k.)** Monitor and control inbound and outbound network traffic through technologies such as firewalls, router policies, IPS, IDS, and host-based security services. |  |
| **l.)** Apply security patches in a timely manner (preferably within 30 days of release). |  |
| **m.)** Is there Security Awareness Training for handling FOUO? |  |
| **n.)** How will data spills of classified information be handled. |  |
| **Table is Unclassified** | |

*5.5 (U) Offeror Comments (Provide any comments that would clarify how the IT system operates or any future plans to address any area discussed in this form):*

# (u) nro aUTHORIZED CLASSIFIED INFORMATION SYSTEM DESCRIPTION

|  |  |
| --- | --- |
| Information System Authorized (Current ATO) | Yes  No |
| Information System Name: |  |
| XACTA Asset Number: |  |
| Information System Authorizing Agency: |  |
| Information System ATO Expiration: |  |
| **Table is Unclassified** | |

**Thank you for completing the ISSA.**

**Please save and submit the final document in Adobe Acrobat Reader (PDF) format.**