SECURITY IMPACT ANALYSIS

Organization:	
System UID:	
Location:	
Date:	
ISSO/ISSM Signature:	
PM Signature:	
SCA Signature:	
AO Signature	

NOTE: AO signature is only mandatory when the SCA determines the requirement

SCA/SCAR Determination/Recommendation(s):

CONTACTS

Information System Security Officer (ISSO)	
Name:	
Phone:	
Email:	
Information System Security Manager (ISSM)	
Name:	
Phone:	
Email:	
Government SAP Security Officer (GSSO)	
Name:	
Phone:	
Email:	
Program Manager (PM)	
Name:	
Phone:	
Email:	
Program Security Officer (PSO)	
Name:	
Phone:	
Email:	
Security Control Accessor (SCA)	
Name:	Jesus Flores
Phone:	661-277-8193 (DSN 527)
Email:	jesus.flores.17@us.af.mil
Authorizing Official (AO)	
Name:	Eileen A. Bjorkman
Phone:	661-277-4366 (DSN 525)
Email:	eileen.bjorkman.1@us.af.mil

Table 1: Initiative/Release Background

Initiative/Release Name	
Project Type	(Examples only: New Development: [insert description] or Enhancement: [insert description] or Maintenance: [insert description]) - REMOVE WHEN SUBMITTING
Type of System	☐ Standalone ☐ Isolated LAN ☐ LAN ☐ WAN
System Changes	
Security Risks	
Planned Deployment Initiation Date	
Planned Deployment Completion Date	
Current Security Categorization of Impacted System(s)	

Table 2: Initiative/Release Description and Potential Security Issues

What are the mission requirements/justification driving the change?
What is the mission impact(s) if not approved?
Please provide a description of the proposed change(s), including ALL additions, deletions, and modifications.
Is the Technical Lead and/or Project Lead aware of any potential security-related issues or challenges associated with this change? If so, briefly describe them or provide and attachment describing them. A vulnerability check needs to be performed to determine known vulnerabilities. The vulnerability websites on the last page are an example for researching known vulnerabilities.
Actions taken to mitigate any known vulnerabilities:

Table 3: Change Type Worksheet

Change Type	Applicable? (Mark X if Applicable)	Description (If Applicable)
New network device(s) (e.g., router, switch, firewall, VPN gateway)	☐	
New server(s)	☐	
New workstation(s) (desktops or laptops)	☐	
Other new HW	☐	
Decommissioning of existing HW	☐	
New virtual server	☐	
New OS	☐	
Upgrade of existing OS	☐	
New COTS application	☐	
Upgrade or patch of COTS application	☐	
New custom application	☐	
Upgrade or bug fix for existing custom application	☐	
New DBMS (e.g., Microsoft SQL Server or Oracle)	☐	
Upgrade of existing DBMS (e.g., Oracle 9i to 10g)	☐	
Addition of new DB instance	☐	
Modification of an existing DB instance (e.g., changes to a table)	☐	
New or upgraded Middleware application or service	☐	
Modifications to ports, protocols, and services used or provided by the system	☐	
Changes intended to address security requirements or improve/modify the security of the system (e.g., cryptographic modules, security patch, authentication, authorization, role changes)	☐	
New information type processed, stored, or transmitted on the system	☐	
Interface change (addition/removed)	☐	
Change of location	☐	
Addition of new Program Identifier (PID) *Note* Addition of a new PID requires SAPCO approval.	☐	

Table 4: Additional Software Information
(If more than one software or application request is required, complete additional software information for each item – See continuation sheet)

Software Title and Version	
Manufacturer/Developer	
Software Features (What functions does it perform?)	
Description of Use (What will it be used for? If it will be modified, state what features will be modified and who will do it.)	
Type of Change (see below for definitions)	☐ Security-Relevant Change (Select an option below. Requires AO Approval) ☐ Security Enforcing ☐ Security Supporting ☐ Security Non-Interfering ☐ Non-Security-Relevant Change (Submit for Informational Purposes Only)
Justification for Type of Change	
Type of Software (Check all that apply)	☐ Commercial Off The Shelf (COTS) ☐ Government Off The Shelf (GOTS) ☐ Freeware ☐ Shareware ☐ Open Source ☐ Locally Developed ☐ Foreign Owned/Developed
If foreign developed, provide alternative US manufactured software, if available, and justification for not using US developed software.	
If freeware, shareware, or open source, provide alternative COTS software, if available, and justification for not using COTS software.	
Source of software	☐ Purchased media (i.e. CD, DVD, etc.) ☐ Download (URL): ☐ Other (Describe):
Is the software on a DoD Approved Products List?	☐ No ☐ Yes – Provide link or certification:
Other Software Dependencies (Is additional software that is not part of the installation package required to be installed:	☐ No ☐ Yes - List required software below:

Table 5: Testing Worksheet

Please describe the tests that will be conducted against the change(s)?

Security Relevant – any hardware or software that is "security enforcing," "security supporting," or "security non-interfering" which can affect an IS's configuration, functionality, or users' privileges, and has the potential to change the risk imposed on the IS.

- **Security Enforcing** – Operating System (OS), access control applications, audit applications, device control applications, second party applications that perform IA, account management, anti-virus, firewall; capable of making changes to the security substructure of the system: modifies a user's account or changes permissions on objects such as enforcing Discretionary access Control (DAC), Mandatory Access Control (MAC), Network Access Control (NAC).
- **Security Supporting** – Impacts a security process or procedures: e.g., software used to perform technical review for AFT; software that is only used by privileged users of the system in the performance of their duties; removing a backup server which may affect availability; code or script that authenticates the user and determines authorization.
- **Security Non-Interfering** – Does not enforce or support any aspect of the system security policy, but due to its presence inside the security boundary, e.g., code running a privileged hardware mode within the OS, risk is elevated.

Table 6: SECURITY IMPACT WORKSHEET

Control Family	Explanation	Yes	No	Description
AC	Will change(s) to system effect how the system limits: (i) information system access to authorized users, processes acting on behalf of authorized users or devices (including other information systems); and (ii) the types of transactions and functions that authorized users are permitted to exercise.	☐	☐	
AT	Will change(s) affect required system training to ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities?	☐	☐	
AU	Will change(s) affect how system audit requirements to (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	☐	☐	
CM	Will change(s) to the system impact the (i) baseline configuration and inventory of organizational information systems; (ii) establishment and enforcement of security configuration settings; and (iii) ability to monitor and control changes to the baseline configurations and to the constituent components of the systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycle.	☐	☐	
IA	Will change(s) to the system impact how it (i) identifies users, processes acting on behalf of users, or devices; and (ii) authenticates (or verifies) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	☐	☐	
MA	Will change(s) to the system impact how (i) periodic and timely maintenance is performed; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.	☐	☐	
MP	Will change(s) to the system impact how (i) information contained in the systems in printed form or on digital media is protected; (ii) access to information in printed form or on digital media removed from the systems is limited to authorized users; and (iii) how digital media is sanitized or destroyed before disposal or release for reuse.	☐	☐	

PE	Will change(s) to the system/system environment change how (i) physical access to information systems, equipment, and the respective operating environments is limited to authorized individuals; (ii) the physical plant and support infrastructure for information systems is protected; (iii) supporting utilities for information systems is provided; (iv) and (v) appropriate environmental controls in facilities are provided.	☐	☐	
SC	Will change(s) to the system effect how: (i) communications (i.e., information transmitted or received by organizational information systems) are monitored, controlled, and protected at the external boundaries and key internal boundaries of the information systems; and (ii) architectural designs, software development techniques, and systems engineering principles that promote effective information security are implemented.	☐	☐	
SI	Will change(s) to the system effect how (i) system flaws are identified, reported, and corrected in a timely manner; (ii) malicious code protection is employed; (iii) system events are monitored and detected; (iv) the correct operation of security functions is verified; and (v) information is checked for accuracy, completeness, validity, and authenticity.	☐	☐	

Table 4 Continuation Sheet: Additional Software Information
(Copy Table for each software/application requested)

Software Title and Version	
Manufacturer/Developer	
Software Features (What functions does it perform?)	
Description of Use (What will it be used for? If it will be modified, state what features will be modified and who will do it.)	
Type of Change (see below for definitions)	☐ Security-Relevant Change (Select an option below. Requires AO Approval) ☐ Security Enforcing ☐ Security Supporting ☐ Security Non-Interfering ☐ Non-Security-Relevant Change (Submit for Informational Purposes Only)
Justification for Type of Change	
Type of Software (Check all that apply)	☐ Commercial Off The Shelf (COTS) ☐ Government Off The Shelf (GOTS) ☐ Freeware ☐ Shareware ☐ Open Source ☐ Locally Developed ☐ Foreign Owned/Developed
If foreign developed, provide alternative US manufactured software, if available, and justification for not using US developed software.	
If freeware, shareware, or open source, provide alternative COTS software, if available, and justification for not using COTS software.	
Source of software	☐ Purchased media (i.e. CD, DVD, etc.) ☐ Download (URL): ☐ Other (Describe):
Is the software on a DoD Approved Products List?	☐ No ☐ Yes – Provide link or certification:
Other Software Dependencies (Is additional software that is not part of the installation package required to be installed:	☐ No ☐ Yes - List required software below:

VULNERABILITY CHECK WEBSITES

This list IS NOT all inclusive, but is a starting point for the due diligence process.

- NIST National Vulnerability Database (NVD): http://web.nvd.nist.gov/view/vuln/search
- US-CERT Vulnerability Notes Database: http://www.kb.cert.org/vuls/
- US-CERT Vulnerability Current Activity: https://www.us-cert.gov/
- Common Vulnerabilities and Exposures: http://cve.mitre.org/cve/
- Common Weakness Enumeration: http://cwe.mitre.org/
- Common Attack Pattern Enumeration and Classification - https://capec.mitre.org
- DoD Information Assurance Vulnerability Management (IAVM) Program (requires CAC) - https://iavm.csd.disa.mil/
- CVE Details - http://www.cvedetails.com
- Intelink Software APL: https://intelshare.intelink.gov/sites/afisra-a6s/a6sc/Lists/APL/AllItems.aspx
- Cisco Security Advisories: https://tools.cisco.com/security/center/publicationListing.x

AF EPL Site: https://usaf.dps.mil/teams/EAO/Lists/COTSGOTS%20Software/Reciprocity.aspx
NIAP Validated Products: https://www.niap-ccevs.org/CCEVS_Products/pcl.cfm
CC Certified Products: http://www.commoncriteriaportal.org/products
DoD Unified Capabilities APL (need CAC): https://aplits.disa.mil/processAPList.action