**Information Technology Categorization Section Checklist**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. ***System General Information*** | | | | | | | | | | | | | | | | | | |
| AF ID: <L-XXXXX>  AF IT: <Insert the official system name, e.g., F-15E Strike Eagle> | | | | | | | | | | | | | | | | | | |
| 1. ***System Purpose/Mission/Data Processed/Stored*** | | | | | | | | | | | | | | | | | | |
| The purpose of L-XXXXX is…  The mission supported is…  Data processed and stored includes…  *<Tell a story here so the AO understands what your system does>* | | | | | | | | | | | | | | | | | | |
| 1. ***Authorization Boundary*** | | | | | | | | | | | | | | | | | | |
| AETC RT&E  AF Enterprise  AFMC DTE  AFOTEC  Aircraft  Civil Engineering | Civil Engineering (ICS)  Command and Control  DC3  Finance  Industrial Depot Maint.  Logistics | | | | | | | | Nuclear  Nuclear (non-NC3)  OTI/LVC  Rapid Cyber Acquisition  Special Access Programs (SAP)  Science & Technology | | | | | | | | | SFS/LE  Space  USAFA  Weapons |
| 1. ***Classification Information*** | | | | | | | | | | | | | | | | | | |
| Highest Data Classification: (Example: Top Secret / Secret / Confidential / Unclassified) [include caveats] | | | | | | | | | | | | | <SECRET//SAR-XXX> | | | | | |
| Releasability (Example: NOFORN / NATO / FVEY | | | | | | | | | | | | | <NOFORN, HVSACO> | | | | | |
| Security Classification Guide (SCG) Reference: [include all] | | | | | | | | | | | | | <Include SCG reference for each PID on your system> | | | | | |
| 1. ***User Information*** | | | | | | | | | | | | | | | | | | |
| Any Foreign National users? | | | | | | | | | | | | | Yes  No | | | | | |
| Do all users have the formal access for all data? | | | | | | | | | | | | | Yes  No | | | | | |
| System Protection Level (reference JSIG)  (Accessibility Overlay required for PL-3, PL-5, and PL-5 systems) | | | | | | | | | | | | | PL-1  PL-2  PL-3  PL-4  PL-5 | | | | | |
| 1. ***CNSS Overlay Questions*** | | | | | | | | | | | | | | | | | | |
| Does the information system contain PII or PHI? (Reference CNSSI 1253F, Attachment 6)  If the answer is no, then Privacy Overlays do not apply.  If yes, then a Privacy Impact Assessment (PIA) must be completed. | | | | | | | | | | | | | Yes  Low  Moderate  High  No | | | | | |
| Cross Domain Solution Overlay: Will you implement, manage, or maintain a Cross Domain Solution? (Refer to CNSSI 1253F, Attachment 3) | | | | | | | | | | | | | Yes (CDS Overlay is required)  No | | | | | |
| Intelligence Overlay: Does the system process, store, or transmit ISR? (Refer to CNSSI 1253, Attachment 4) | | | | | | | | | | | | | Yes (Intelligence Overlay is required)  No | | | | | |
| Classified Information Overlay: Does the system process, store, or transmit classified information? (Refer to CNSSI 1253, Attachment 5) | | | | | | | | | | | | | Yes (Classified Information Overlay is required)  No | | | | | |
| Nuclear Command and Control (NC3) Overlay: Does the system store, process, or transmit NC3 data? | | | | | | | | | | | | | Yes (Classified Information Overlay is required. AF IC recommends INT-A)  No  \*NOTE: utilization of the NC3 Overlay also requires the implementation of the Intel C and Classified Overlays | | | | | |
| Is the system (or subsystem) a space platform as defined in CNSSP No. 1253 and unmanned? (Refer to CNSSI 1253F, Attachment 2) | | | | | | | | | | | | | Yes (Space Platform Overlay is required)  No | | | | | |
| Mission/Function Specific Overlay: Is your system required to execute a mission or function-special overlay? (e.g., Financial, Acquisition) | | | | | | | | | | | | | Yes (Specify Overlay and OPR)  Overlay 1:  Overlay 2:  No | | | | | |
| 1. ***Categorization Information*** | | | | | | | | | | | | | | | | | | |
| **Categorize the CIA for APPLICABLE Information Types (i.e., Low, Moderate, or High).** | | | | | | | | | | | | | | | | | | |
| **Information Types** | | | **Confidentiality** | | | | **Integrity** | | | | **Availability** | | | | **Justification** | | | |
| **L** | | **M** | **H** | **L** | **M** | **H** | | **L** | **M** | | **H** |
| <Insert Information Type: see NIST 800-60Vl&V2>  <Look at V2 for recommended categorization levels. When selecting data types from NIST 800-60 publications, ensure the CIA verbiage for the selected data type matches the justification used for the system. Many of the Test Center systems can use D.20.1 for Research and Development Information Type.> | | |  | |  |  |  |  |  | |  |  | |  | <STRONG JUSTIFICATION IS NEEDED FOR APPROVAL. Must show justification for each info type on Confidentiality, Integrity, and Availability. See last page of this template for questions you should answer to complete this section.>  <Samples>  **CONFIDENTIALITY:** The data collected measures performance and potential vulnerabilities of System Under Test (SUT). Exposure of this data could have serious impacts to operational use of these systems. JSIG Section 2.3.1.1 mandates that all information systems processing classified SAP data be categorized with a minimum confidentiality impact level of Moderate. The ISO with concurrence of the AO has determine that no escalation of confidentiality impact is warranted.  **INTEGRITY:** The data collected for this system is test and evaluation data, which if modified, could destroy delivery times by loss of design and development work. Historical program decisions and continuity would be lost and require duplication of efforts to regain capability. Alterations of this data could lead to false knowledge being propagated resulting in incorrect program decisions. The labor costs to recreate design documents could be 1significant. If an adversary modified or deleted our data, it could produce negative impacts to the schedule, costs, and technical capabilities which could influence the requirement for higher level decisions and funding. The consequences of unauthorized  modification or destruction of most research and development information can be seriously disruptive to the progress of research activities; therefore, the Integrity im2,act level is Moderate.  **AVAILABILITY:** The unavailability of access to or use of any information processed, stored, and transmitted by this system may be a hindrance but i would have limited adverse effect on organizational operations, organizational assess, individuals, or other organizations, or the national security interest of the United States as  the data is not considered to be mission essential and can be accessed from alternate locations in the event personnel were directed to evacuate.  Therefore, the impact to the system's availability is Low. | | | |
| <Insert Information Type: see NIST 800-60Vl&V2> | | |  | |  |  |  |  |  | |  |  | |  | <Justification is needed for each information type.> | | | |
| FINAL SYSTEM CATEGORIZATION | | |  | |  |  |  |  |  | |  |  | |  |  | | | |
| NOTES: In the table above, be sure to add main information type category above the specific information types. For any deviation from the provisional recommended Security Categorization for each information type, per NIST 800-60, add comments in the Justification column. Final row should represent the overall categorization based on a High Water Mark. | | | | | | | | | | | | | | | | | | |
| 1. ***Proposed Information Technology (Check One)*** | | | | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | | | | |
| **Information Systems** | | **Platform IT** | | | | | | | | | | **IT Services**  **(Assess Only)** | | | | | **IT Products**  **(Assess Only)** | |
| Major Application  Enclave | | PIT Systems  PIT Subsystem(s) (Assess Only)  PIT Component(s) (Assess Only) | | | | | | | | | | Internal  External | | | | | Software  Hardware  Applications | |
| 1. ***RDT&E (Check One if Applicable)*** | | | | | | | | | | | | | | | | | | |
| Zone A | | Zone B | | | | | | | | Zone C | | | | | | Zone D | | |
| 1. ***Describe the System Boundary*** | | | | | | | | | | | | | | | | | | |
| Provide a detailed boundary drawing that clearly shows the cybersecurity authorization boundary. Identify any external interfaces to the IT in this section. An external interface is any interface that crosses the authorization boundary. Indicate all information exchanges such as removable media, media for system updates, RF, Ethernet WiFi, etc. If the system has no external interfaces, clearly state that in this section.  <Sample Isolated Network>  <Sample Network with External Connection>  <Sample Standalone Workstation> | | | | | | | | | | | | | | | | | | |
| The DAF IT Categorization and Selection Checklist was completed by a team of personnel consisting of <ISSO, ISSM, PM/ISO, SysAdmin>. The overall Impact Analysis, Security Control Baseline selection, and required overlays were determined after a thorough review. | | | | | | | | | | | | | | | | | | |
| 1. ***System Owner/Mission Owner/Government Representatives*** | | | | | | | | | | | | | | | | | | |
| Title | | | | Name | | | | | | | | Phone | | | | | Organization | |
| ISSO: | | | |  | | | | | | | |  | | | | |  | |
| PM: | | | |  | | | | | | | |  | | | | |  | |
| ISSM: | | | |  | | | | | | | |  | | | | |  | |
| ISSE: | | | |  | | | | | | | |  | | | | |  | |
| User Representative: | | | |  | | | | | | | |  | | | | |  | |
| Requirements Lead: | | | |  | | | | | | | |  | | | | |  | |
| Security Control Assessor: | | | | Jesus Flores | | | | | | | | DSN 527-8193 | | | | | 412 TW/IPIM | |
| Authorizing Official: | | | | Dr Eileen Bjorkman | | | | | | | | DSN 527-4436 | | | | | AFTC/CA | |
| SAP CIO | | | | AF SAP CIO (CORE) or mailto:  [SAF.CNSZ.Mailbox@us.af.mil](mailto:SAF.CNSZ.Mailbox@us.af.mil) | | | | | | | |  | | | | | SAF/CNSZ | |
| 1. The program office/ISO will integrate cybersecurity and cybersecurity risk management into their overall systems engineering, acquisition, test and evaluation, and risk management process. 2. The program office/ISO will complete Risk Management Framework (RMF) steps to obtain an Interim Authority to Test (IATT) or Authority to Operate (ATO), as appropriate, before system testing or operations commence. 3. For AF SAP IT systems, the program office/ISO will ensure the system is registered in the AF SAP Inventory and coordinated through the MAJCOM POC. | | | | | | | | | | | | | | | | | | |
| ***RMF ACTION*** | | | | | | | | | | | | | | | | | | |
| Assess & Authorize  Assess Only | | | | | | | | | | | | | | | | | | |

1st Ind, Program Manager MEMORANDUM FOR RECORD

I have reviewed and agree with the impact values and required overlays listed above.

Include Name, Rank/Grade, Position and Organization

2d Ind to Air Force (AF) Information Technology (IT) Categorization and Selection Checklist Boundary Authorizing Official

MEMORANDUM FOR RECORD

I have reviewed and agree with the impact values and required overlays listed above.

EILEEN A. BJORKMAN, SES, DAF

Executive Director, Air Force Test Center

**DELETE THIS SECTION WHEN SUBMITTING**

A loss of *confidentiality* is the unauthorized disclosure of information. (WHAT IMPACT WOULD IT HAVE IF YOUR SAP INFORMATION WAS ACCESSED BY AN UNAUTHORIZED INDIVIDUAL?)

A loss of *integrity* is the unauthorized modification or destruction of information. (WHAT IMPACT WOULD IT HAVE IF YOUR INFORMATION WAS MODIFIED OR DESTROYED? IF UNAUTHORIZED MODIFICATION OF YOUR DATA WAS RELEASED AND USED, WHAT IMPACT WOULD THAT HAVE)

Integrity is looked at closely if the impact level is LOW so you must have strong justification. Some more things to think about:

For test data, would unauthorized modification or deletion affect future research and development? Would there be a significant cost if the program data was lost or tampered with?

If an adversary were able to destroy or modify our data, how much harm would that incur towards our organization and mission? Would it influence higher level decisions or funding?

A loss of *availability* is the disruption of access to or use of information or an information system. (WHAT IMPACT WOULD IT HAVE IF YOUR INFORMATION/DATA WAS UNAVAILABLE FOR A PERIOD OF TIME?)

The *potential impact* is **LOW** if-

* The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability 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.

The *potential impact* is **MODERATE** if-

* The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability 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.

The *potential impact* is **HIGH** if-

* The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability 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.