|  |  |  |  |
| --- | --- | --- | --- |
| **A4 Information Technology (IT) Categorization and Selection Checklist (ITCSC)**  **v1.61 (8 Feb 2021)** | | | |
| ***1. System Identification Information***  *Input values for the IT, as applicable. Refer to ITIPS and eMASS for values being provided.* | | | |
| 1A. | IT Name:\* | *Get this from the eMass “System” tab: “System Name:” field* | |
| 1B. | IT Acronym:\* | *Get this from the eMass “System” tab: “System Acronym:” field* | |
| 1C. | IT Version:\* | *Get this from the eMass “System” tab: “* *Version / Release Number:” field* | |
| 1D. | ITIPS ID: | TBD | |
| 1E. | DITPR ID: | N/A | |
| 1F. | eMASS ID: | *Get this from the eMASS “System” tab: “* *System Identification:” field* | |
| ***2. Technical Description/Purpose\****  *Provide a description of the function and purpose of the system (e.g. data analysis, network support, logistics, and administration) Identify any mission critical functions supported by the IS. Describe the primary computing platforms(s) used (e.g. mainframe, desktop, LAN, WAN). Mission Apps should also include a general description of the principal IS components including hardware, software and communication resources.* | | | |
| *•What is the purpose of the IT/OT?*  *Describe the purpose of BOTH the OT and the IT.*  *For example: “The OT provides automated control of the ambient temperature of x buildings. The IT provides historical data storage, thermostat control services, data display and remote access services”*  *What is the system – specific to the base not a just generic FRCS type description?*  *Where is the system – what buildings / areas / section of the base does it support?*  *How many buildings make up the control system?*  *Ensure to document the primary and any alternate locations and identify any operations centers, control centers, dispatch centers, etc. for the control system.*  *Document any redundancy and alternate means to operate, configure, or maintain the control system.*  *•Is the IT mission essential to the warfighter?*  *What is used to determine mission criticality?*  *DoD 8580.1 Acquisition document - E.2.1.15 & E.2.1.16:*  *- Mission Support*  *- Mission Essential*  *- Mission Critical*  *What does the system do that makes it essential to the warfighter?*  *When assessing the control system as mission essential, ensure to document the rationale for the assessment of mission support or mission essential or mission critical.*  *What does the control system do that makes it mission essential to the warfighter?*  ***NOTE:*** *IF a Critical Infrastructure Vulnerability Assessment (CICVA) has been accomplished for the system and has identified the system as a Mission Critical Control System (MC-FRCS) and a National Manager for NSS Advisory Memo - Security of MC-FRCS loaded to artifacts in the eMASS package, the mission criticality of the CECS is at least Mission Essential regardless of control system function.*  *•What are the major hardware/software components of the IT/OT?*  *Ensure* ***every component*** *identified on the topology diagram is described here according to the following guidance:*  *Hardware / Software components – what makes up the system is in terms of hardware and software: include make/model/operating system/ and major functional software applications?*  *Functional components (Command Post / Control Center / Dispatch Location) and hardware software that makes them up.  Major hardware software components that make up the system.  FRCS vendor.  Server hardware and software.  Major OEM components (SCADA / Controllers / PLCs).  Workstations – PCs / tablets / touchscreens, etc.*  *Document the number of machines, operating systems, connectivity, network description (e.g. closed loop fiber interconnected via Level 3 managed switches), and functional hardware and software that make up the control system.*  *Describe what the servers (where applicable) and workstations functions are.*  *Describe the purpose of all identified hardware, e.g. switches, modems, printers (if applicable), and RF transceivers/transmitters/receivers.*  *Describe what devices are used and how the system is interconnected.*  *•What services are provided by the IT/OT, and are any of those services publicly accessible (can anyone access information contained on the IT without needing authorization)?*  *Who uses the system, and what do they use it for.*  *For systems that have a connection to the Internet or transmits RF signals, ensure to document security features that mitigate or potentially mitigate public accessibility.*  *Describe the encryption and any other security measures in place to prevent unauthorized public access.*  *•How will each of the Information Types be stored, processed, and/or transmitted by the IT/OT?*  *Information types stored, processed, transmitted – User information (if applicable) and system data.*  *Where is it collected,*  *Where is it transmitted to,*  *How is it transmitted there,*  *What is done with it there (processed),*  *Where is it stored (server database), for how long?*  *•If the IT is undergoing a significant modification, describe the modification and its purpose, otherwise ignore this requirement.* | | | |
| ***3. Information Technology Topology\****  *Describe the IT/OT Boundary. For external interfacing systems, include a detailed boundary drawing (DoDAF OV-1 and SV-1 minimum). IT/OT topology should provide a brief description of the applets, subsystems, modules that comprise the IT/OT. If applicable, identify the communication interfaces external to the IS.* | | | |
| 3A. | Topology Description | | *Use this space to describe the topology below e.g. “The XYZ system uses C1 as the hosting enclave and GCDS for primary authentication, it allows for public internet access to the web interface but administrators must use the client and system interfaces must use FTPS.”*  *High level description without repeating everything from section 2.  Detail anything in the topology that isn’t obvious that is not already explained above.* ***Explain to someone who is not technical*** *what the topology diagram is showing.*   * *Document the interconnections between major components* * *Identify specific network devices and their functions* |
| 3B. | Topology Diagram (OV-1, SV-1) | | |
|  | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***4. Information Technology Type\****  *Select from list below* | | | | | | |
| Platform IT - PIT System | | | | | | |
| ***5. Authorizing Official & Authorization Boundary\****  *Select from list below. A list of AOs and description of their boundaries can be found on the Air Force Risk Management Framework (RMF) Knowledge Service (KS) at:* [*https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/AirForce/Pages/default.aspx*](https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/AirForce/Pages/default.aspx) | | | | | | |
| Civil Engineering (CE) | | | | | | |
| ***6. Categorization Information\****  *Enter Information Types processed by the IT/OT and choose the applicable security requirement (REF:NIST SP 800-60 Vol 1 & II )* | | | | | | |
| **6A. Information Types** | | **Confidentiality** | **Integrity** | **Availability** | | **Justification** |
| (replace this) C.x.x.x – Information Type | | Low | Moderate | Low | | *Categorization is about the impact to the mission, facilities, etc. when system compromised has occurred*  *Identification to the impact to the mission, people, equipment, finances, etc. what is the impact when the compromise occurs?*  ***DO NOT*** *document alternate means of operation, any mitigations of risk or likelihood of occurrence of an incident in this section.*  *Describe the data processed, stored or transmitted and the impact on the mission when compromised for confidentiality, integrity and availability. What is the level of adverse effect and level of damage?*  *NIST 800-60, it identifies a baseline categorization, further verbiage identifies*  *Justifications should be in specific terms of impact to the base mission and not just cut and pasted impact statements from the guidance documentation.*  *FIPS 199 Table 1, Potential Impact Definitions for Security Objectives*  *Assessment of Adverse Effect:*  *Low - Limited adverse effect,*  *Moderate - Serious adverse effect,*  *High - Severe or Catastrophic adverse effect?*  *Assessment of Damage:*  *Low - Minor damage,*  *Moderate - Significant damage that* *does not involve loss of life or serious life threatening injuries*  *High - Major damage, Severe or catastrophic harm involving loss of life or serious life threatening injuries*  *When confidentiality of the data is compromised (unauthorized disclosure), what is the impact to the mission?*  *When integrity is compromised (unauthorized disclosure), what is the impact to the mission?*  *When availability is compromised (loss of access to information), what is the impact to the mission?*  *Describe the specific data in the system that best describes these information types and a justification on all selected CIA impact values e.g.*  *“ This data type processed by the system shows all the Money spent on LOG IT and where it was spent. Confidentiality:*  *The confidentiality is low because the data we utilize is publicly accessible and there will be limited impact to the mission financially if an adversary was able to read our information since it can be viewed by anyone.*  *Integrity:*  *There will be a serious impact to the mission if people were able to change the values in the system as it is the authoritative source for the funds spent on Log IT. False data may incur investigation through the IG or other auditors, causing a waste in time and resources for the AF.*  *Availability:*  *The system can be down for months at a time as financial audits are performed only annually. Only an outage beyond a year will cause any impact to the mission and even then it will likely be limited as audits are sparse and not mandatory.”* |
| replace this) C.x.x.x – Information Type | | Low | Moderate | High | |  |
| Click or tap here to enter text. | | Choose an item. | Choose an item. | Choose an item. | | *When all Information Types have been identified, categorized and justification provided; Remove unused table rows.* |
| Click or tap here to enter text. | | Choose an item. | Choose an item. | Choose an item. | |  |
| Click or tap here to enter text. | | Choose an item. | Choose an item. | Choose an item. | |  |
| Click or tap here to enter text. | | Choose an item. | Choose an item. | Choose an item. | |  |
| Click or tap here to enter text. | | Choose an item. | Choose an item. | Choose an item. | |  |
| **6B. IT/OT CATEGORIZATION** *(Apply ‘high water mark’ for each column or provide justification)* | | Low | Moderate | High | | *Describe any special factors that the aggregation of the data type can create especially if it changes CIA impact values, othewise use the highest water mark e.g. “Aggregating these data types makes this information system NSS and can cause catastrophic damage to the AF mission if an adversary was able to access all the information.”*  *The highwater mark for the ALCS or EMCS or AMRS, etc. is L/M/M, or L/L/L, or M/M/M, etc. based on the D.7.1 or D.7.2 or D.11.3 or D.16.5, etc. and C.3.1.1 information types per NIST SP 800-60, FIPS 199 and index NN of the Distribution of Facility-Related Control Systems Master List memo dated 10/19/2020 Attachment – A: “Facility Related Control System (FRCS) Master List Final” dated 11/15/2020, was used to identify the FRCS and assess CIA baseline dependent upon mission criticality classification.*  ***IF a CICVA has been accomplished on the system****, add the following statement:*  *“A CICVA assessment exists for this system. Per the National Manager for NSS Advisory Memo - Security of MC-FRCS loaded to artifacts in the eMASS package for this system, the baseline CIA values for these systems should be set at Mod/Mod/Mod."* |
| ***7. Overlays\****  *Overlays would only be required in very rare circumstances.* | | | | | | |
| 7A. | *Intelligence Overlay:* Does the IT/OT process, store, or transmit ISR? Ref: (e) | | | | Yes (Intelligence Overlay is required)  No | |
| 7B*.* | *Cross Domain Solution Overlay*: Will you implement, manage, or maintain a Cross Domain Solution? Ref: (d) | | | | Yes (CDS Overlay is required)  No | |
| 7C. | Nuclear *Command, Control & Communications (NC3) Overlay:* Does the IT/OT store, process or transmit NC3 data?  NOTE: use of the NC3 Overlay also requires the implementation of the Intel non-NC3 Ref: (n, e) | | | | Yes (NC3 Overlay is required)  No | |
| 7D. | *Space Platform Overlay:* Is the IT/OT (or subsystem) a space platform as defined in CNSSP No. 1253 and unmanned? Ref: (c) | | | | Yes (Space Platform Overlay is required)  No | |
| *7E.* | *Classified Information Overlay:* Does the IT/OT store, process, or transmit classified information?  Ref: (f) | | | | Yes (Classified Information Overlay is required)  No | |
| *7F.* | *Privacy Overlay:* Does the IT/OT store, process, or transmit Personally Identifiable Information or Private Health Information? (e.g. Social Security Number, Health records  Ref: (g) | | | | Yes (Privacy Overlay is required)  No | |
| *7G.* | *Financial (FIAR) Overlay:* Does the IT/OT store, process, or transmit Financial information Ref: (w) | | | | Yes (FIAR Overlay is required)  No | |
| *7H.* | *Mission/Function Specific Overlay:* Is your IT/OT required to execute an organizational mission or function-special? (E.g. Acquisition etc.) Ref: (h) | | | | Yes  Overlay: Click or tap here to enter text.  OPR: Click or tap here to enter text.  No | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ***8. National Security System Designation\****  *Refer to the NSS Questionnaire referenced in NIST SP 800-59, then complete this section.* | | | | | | |
| 8A. | Have you completed the NSS questionnaire?  *Refer to NIST SP 800-59. All systems must complete the questionnaire, however signatures are only required if the system IS designated NSS.*  *All systems require a completed NSS.*  Upload the completed NSS questionnaire to eMass as a supporting artifact | | | | Yes  No | |
| 8B. | Is this a National Security System (NSS)?  *NOTE: If the answer to any of the six questions in the NSS Questionnaire is “yes”, then the system is a national security system.* | | | | Yes  No | |
| ***9. Cloud Computing\**** | | | | | | |
| 9A. | Is the IT going to be utilizing cloud-hosted services? | | | | Yes  No | |
| 9B. | What is the Cloud Information Impact Level required for the IT?  *Information Impact Level is determined whether you are in the cloud or not. This will help guide interfacing to cloud systems and future migrations. Refer to the DoD CC SRG (*[*link*](https://dl.dod.cyber.mil/wp-content/uploads/cloud/pdf/Cloud_Computing_SRG_v1r3.pdf)*)* | | | | IL2 (Public)  IL4 (CUI)  IL5 (NSS)  IL 6 (Classified)  N/A | |
| 9C. | What Cloud Information Impact Level (IL) are the services rated at?  *Refer to the DoD CC SRG (*[*link*](https://dl.dod.cyber.mil/wp-content/uploads/cloud/pdf/Cloud_Computing_SRG_v1r3.pdf)*) and the DISA Service Catalog (*[*link*](https://disa.deps.mil/ext/CloudServicesSupport/Pages/Catalog-DoD-Approved-Commercial.aspx)*)* | | | | IL2 (Public)  IL4 (CUI)  IL5 (NSS)  IL 6 (Classified)  N/A | |
| 9D. | What cloud service offering type(s) will the IT utilize? (*Check all that apply*) | | | | SaaS  PaaS  IaaS  N/A | |
| ***10. Privacy\****  *Note: For assistance with completing this section please contact your Installation/MAJCOM Privacy Officer* | | | | | | |
| 10A. | | Have you completed a Privacy Impact Assessment (PIA)? *ref (t)*  *Per AFI* 33-332*, all IT \*must\* complete a PIA. If no PII is collected only the PM is required to sign.*  *Instructions for 10A and Ref(t) state PIA is not required for FRCSs.* | | | Yes  No | |
| 10B. | | What is the defined PII Impact level? *ref (t)* | | | Low  Mod  High  N/A | |
| ***11. Major Roles/Points of Contact\****  *The AF RMF IT Categorization and Selection Checklist was completed by the RMF Team named below. Impact analysis, Security Control Baseline selection, and required overlays have been identified, reviewed and certified. Representatives denoted with an asterisk (\*) are mandatory.* | | | | | | |
| **Title** | | | **Name** | **Phone (DSN)** | | **Organization** |
| Authorizing Official:\* | | | Ms. Nancy J. Balkus, SES | 223-4078 | | AF/A4C |
| AODR: | | | Mr. Peter Tresnak, GS-15 | 223-3519 | | AF/A4CS |
| Program Manager\* | | | REQUIRED INFORMATION | xxx-xxxx | | AF/xxxx |
| SCA:\* | | | Mr. Christopher Correll, GS-13 | 523-6416 | | AFCEC/COOI |
| ISSM:\**Cannot be blank* | | | REQUIRED INFORMATION | xxx-xxxx | | AF/xxxx |
| Functional Lead: | | | N/A | N/A | | N/A |
| Primacy POC:\* | | | REQUIRED INFORMATION | xxx-xxxx | | AF/xxxx |
| Notes:   1. *The program office/ISO will integrate cybersecurity risk management into their overall systems engineering, acquisition, test and evaluation, and risk management processes.* 2. *The program office/ISO will complete Risk Management Framework (RMF) steps to obtain to obtain the appropriate approval or authorization documentation before IT testing or operation.* 3. *For AF IT (IAW AFI 17-101, Figure 1.1) the program office/ISO will ensure the IT (as applicable) is registered in Information Technology Investment Suite (ITIPS) and Enterprise Mission Assurance Support System (eMASS)* | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **12. Summary\***  *Summary information from the rest of the form. Information in this section should be the same as identified in previous sections of the document.* | | | | | | | | |
| **IT Name:** (1B)  Click or tap here to enter text. | | | | | | | | |
| **ITIPS ID:** (1D)  Click or tap here to enter text. | **DITPR ID**: (1E)  N/A | | | | **eMASS ID**: (1F)  Click or tap here to enter text. | | | |
| **IT/OT Type** (4) | | | | **AO Boundary** (5) | | | | |
| Platform IT - PIT System | | | | Civil Engineering (CE) | | | | |
| **Overlays(7)** | **NSS Questionnaire Complete** (8A) | **Cloud** **Utilization** (9A) | | | **Information Impact Level of Cloud Used** (9C) | | | **PIA Complete** (10A) |
| Financial (FIAR)  Space Platform  Cross Domain Solution (CDS)  Intelligence  Classified  Privacy  Nuclear (NC3)  Mission Specific Overlay  N/A  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Yes | No | | | N/A | | | No |
| **NSS Designation** (8B) | **Information Impact Level Required** (9B) | | | **Cloud Service Offering Type** (9D) | | | **Privacy Impact Level**(10B) |
| No | N/A | | | N/A | | | N/A |
| **IT/OT Categorization** (6) | | | | | | | | |
| **FINAL IT/OT CATEGORIZATION** | **Confidentiality** | | | **Integrity** | | | **Availability** | |
| Choose an item. | | | Choose an item. | | | Choose an item. | |
| **Approval** | | | | | | | | |
| AUTHORIZING OFFICIAL/ DESIGNATED REPRESENTATIVE | | | Peter Tresnak, GS-15 | | | | | |
| Organization: | | | AF/A4CS | | | | | |
| Email: | | | Peter.tresnak@us.af.mil | | | | | |
| Phone (Commercial): | | | 703-693-3519 | | | Phone (DSN): | | 223-3519 |
| **Authorizing Official/ Designated Representative**: (Digital Signature) | | |  | | | | | |
|  | | | | | | | | |
| PROGRAM MANAGER: | | | REQUIRED INFORMATION | | | | | |
| Organization: | | | Site specific information | | | | | |
| Email: | | | Site specific information | | | | | |
| Phone (Commercial): | | | xxx-xxx-xxxx | | | Phone (DSN): | | xxx-xxx-xxxx |
| **Program Manager/ Information System Owner**: (Digital Signature) | | |  | | | | | |

**INSTRUCTIONS**

**Residual evaluations of all data should weigh impact and likelihood in the assessment of all decision based questions in the ITCSC.**

**1. System Identification Information**

System Name: The System Name entered here MUST match the Investment Name being entered during Information Technology (IT) Investment Portfolio System (ITIPS) registration

System Acronym: The same acronym entered in ITIPS as Investment Acronym

Version: Version of the system

**2. Technical Description/Purpose**

Provide a general technical description of the function and purpose of the proposed IT/OT. This description should tell the story of who, what, where, when, why, and how the IT/OT supports the warfighter and/or other IT/OT. Consider the following when filling out this section:

•What is the purpose of the IT/OT?

•Is the IT mission essential to the warfighter?

•What are the major hardware/software components of the IT/OT?

•What services are provided by the IT/OT, and are any of those services publicly accessible (can anyone access information contained on the IT without needing authorization)?

•How will each of the Information Types be stored, processed, and/or transmitted by the IT/OT?

•If the IT is undergoing a significant modification, describe the modification and its purpose, otherwise ignore this requirement.

**3. Information Technology Topology**

3A. Provide a brief narrative that clearly describes the IT/OT system boundary, as well as any external interfaces or information exchanges (removable media, RF, Ethernet, Wi-Fi etc.) that would cross that boundary. If the IT/OT is standalone (no external interfaces), then clearly state that in this section.

3B. Provide an authorization boundary diagram. ***Required DoDAF Artifact***: If external interfaces exist, the follow-on requirement is to generate a detailed and comprehensive boundary drawing (DoDAF OV-1 and SV-1 minimum) and post it to eMASS as an artifact during or subsequent to initial registration.

**4. Information Technology Type**

Distinguishes between Information Systems, PIT Systems, PIT Subsystems, Services, and Components. *See ref:* (v)

**5. Authorizing Official & Authorization Boundary**

A listing of AOs and AO boundary descriptions can be found on the Air Force Risk Management Framework (RMF) Knowledge Service (KS) at: <https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/AirForce/Pages/default.aspx>

**6. Categorization Information**

In the table, be sure to add main Information Type category above the specific Information Types on the left column labeled “Information Types”. On the “Justification” column, **describe the real data from the information system** that corresponds with the data type selected and **provide justification for choosing that data type and why the default impacts align with the impacts to your mission>.** For example, if the system manages “Air Traffic Control Data” but the closest data type is “Air Transportation” describe the **similarities and gaps in CIA impacts**. Additionally**, provide justification for any reduction or increase from the default recommended Security Categorization** for each information type, per NIST SP 800-60 Vol. 1 & 2**, add a detailed justification for the change in the Amplifying Data\* column**. Final System Categorization below should represent the overall categorization based on the highest ranking all categories, or if aggregation warrants change please provide justification as well.

**7. Overlays**

Answer the overlay questions to determine if one is required or not.

**8. National Security System Designation**

Carefully read the NSS Questionnaire referenced in NIST SP 800-59. If the answer to any of those six questions is Yes, then the system is an NSS, and will require an Overlay and a signed NSS questionnaire.  
*See Ref: (i) for more information.*

**9. Cloud**

**9A. Cloud Information Impact Level (IL) Required:**

This is based on the Information being processed in the system

Please see the following sections in the DoD CC SRG for further guidance:

3.2.2 Level 2: Non-Controlled Unclassified Information..................................................

3.2.4 Level 4: Controlled Unclassified Information

3.2.5 Level 5: Highly Controlled Unclassified Information or NSS

3.2.6 Level 6: Classified Information up to SECRET  
*See Ref: (j) for more information.*

**9B. Cloud Hosted**

Is the IT going to be hosted in a cloud environment? If “no,” then continue to Question 10.

**9C. Cloud Information Impact Level (IL) of Service**

This is based on the DISA Provisional Authorization (PA) granted to the Cloud Service Offering (CSO)

Please see the following sections in the DoD CC SRG for further guidance:

3.2.2 Level 2: Non-Controlled Unclassified Information.................................................. 26

3.2.4 Level 4: Controlled Unclassified Information .......................................................... 26

3.2.5 Level 5: Controlled Unclassified Information .......................................................... 28

3.2.6 Level 6: Classified Information up to SECRET ....................................................... 29  
*See Ref: (j) for more information.*

**9D. Cloud Service Type**

Identify the Cloud Service Offering (CSO) types to be utilized IaaS, PaaS, or SaaS. Check all that apply.  
*See Ref: (j) for more information.*

**10. Privacy**

It is highly recommended that you complete the Air Force PII confidentiality Impact Level (PCIL) Categorization Checklist and the Privacy Impact Assessment, to complete the Confidentiality Impact and help fill out this section.

As a reminder, the information in the PCIL comes directly from the Privacy Overlay.

**10A. Does the IT have a Privacy Impact Assessment (PIA)?**

Required for all Information Systems (IS) except Platform Information Technology (PIT), Weapons Systems or Industrial Control Systems.

**10B.** Brief explanation of impact levels if PII is exposed:

* Low- Limited (Minor Harm)
* Moderate- Significant degradation, damage, loss or harm
* High- Severe/Major degradation, damage, loss or catastrophic harm.

*See Ref: (l) for more information*

**11. Major Roles/Points of Contact**

The program office/ISO will integrate cybersecurity risk management into their overall systems engineering, acquisition, test and evaluation, and risk management processes.

The program office/ISO will complete Risk Management Framework (RMF) steps to obtain to obtain the appropriate approval or authorization documentation before IT/OT testing or operation.

For AF IT, the program office/ISO will ensure the IT/OT (as applicable) is registered in Information Technology Investment Suite (ITIPS) and Enterprise Mission Assurance Support System (eMASS) as applicable.

**Summary:**

Aggregation of data should be considered when reviewing this data.

PM will fill their name in their signature block

**REFERENCES**

1. Program managers for all information systems are required to complete a Privacy Impact Assessment (PIA) DD Form 2930 in conjunction with an organizational privacy subject matter expert.
   * In cases where no PII/PHI is present, the PIA will serve as a conclusive determination that privacy requirements do not apply to the system.
   * PIA’s are not required for Platform Information Technology (PIT), weapons systems or industrial control systems.
   * All documentation must be coordinated through the servicing Base and MAJCOM Privacy Manager/Monitor before submission to AF Privacy.
2. CNSSI 1253F Attachment 1, Security Overlay Template
3. CNSSI 1253F Attachment 2, Space Platform Overlay
4. CNSSI 1253F Attachment 3, Cross Domain Solution Overlay
5. CNSSI 1253F Attachment 4, Intelligence Overlay
6. CNSSI 1253F Attachment 5, Classified Information Overlay
7. CNSSI 1253F Attachment 6, Privacy Overlay
8. NIST SP 800-39, March 2011, Managing Information Security Risk: Organization, Mission, and Information System View
9. Additional reference for NSS System Determination
   * Military Critical infrastructure – 10 USC 130 (e)
   * Civilian Critical infrastructure – Critical Infrastructure Information Act of 2002
   * Deployment and troop movement – 10 USC 130 (b)
   * Unclassified nuclear data – 42 U.S.C. § 2162
   * Trade Secrets Act data – 15 U.S.C. §§ 46 (f), 57b-2, 15 U.S.C. §3710a(c)
   * Sensitive PII (medical/HIPPA, personnel – related to sexual assault
   * DoDI 6495.02 especially for restricted reports)
   * The Crime Victim’s Rights Act, 18 U.S.C, Section 3771 (DoD implemented by Article 6b, UCMJ—10 U.S.C., Section 806b)
   * Additional protections may be required by the Cloud SRG
10. DoD Cloud Computing Security Requirements Guide (Cloud SRG)
11. Privacy Act, 1974
12. NIST SP 800-122, April 2010, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
13. For more information on preparing or processing an “Assess Only” package refer to the Air Force RMF Knowledge Service (KS)/AF Assess Only Guidance Folder
14. NC3 Overlay: <https://rmfks.osd.mil/rmf/SiteResources/References/Reference%20Library/NC3_Overlay.pdf>
15. NIST SP 800-66; An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
16. NIST SP 800-171; Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
17. Memo: Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings, dtd 15 Nov 17
18. Memo: Designation of 24AF as CSSP for the Air Force, dtd 1 Nov 18
19. United States Office of Personnel Management, System of Records Notice (SORN) Guide, dtd Apr 2010
20. [ITCSC Privacy Checklist](https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/AirForce/Air%20Force%20Shared%20Document%20Library/Base/Privacy/ITCSC%20Privacy%20Checklist.docx)
21. [The Air Force Privacy Office](https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/AirForce/Pages/Documents.aspx?RootFolder=%2Frmf%2Fcollaboration%2FComponent%20Workspaces%2FAirForce%2FAir%20Force%20Shared%20Document%20Library%2FBase%2FPrivacy&FolderCTID=0x0120008CEFE2A54FED0C4D8435348C1B283FC5&View=%7B0B9A7DF7%2D7FDB%2D49D3%2DA1A0%2D8635318EB31A%7D)
22. DoDI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT) Jul 2017
23. [Financial Improvement and Audit Readiness (FIAR) Guidance](https://comptroller.defense.gov/Portals/45/documents/fiar/FIAR_Guidance.pdf) Apr 2017