Air Force (AF) Risk Management Framework (RMF)
Information Technology (IT) Categorization and Selection Checklist (ITCSC)

1. System Identification Information

System Name: (duplicate in ITIPS)	
System Acronym: (duplicate in ITIPS)	
Version:	
ITIPS (if applicable)	
DITPR# (if applicable)	
eMASS# (if applicable)	

All information systems will need to complete a Privacy Impact Assessment (PIA) in conjunction with an organizational privacy subject matter expert. The PII Confidentiality Impact Level (9H) is a significant contributor to the system categorization and CONFIDENTIALITY level. (Section 10)

2. Technical Description/Purpose

3. Authorizing Official (Check One) & Authorization Boundary

☐ AETC RT&E	☐ Command & Control (C2)	☐ Logistics (AF/A4)	☐ Security Forces (SF)
☐ AF Enterprise	☐ Cyber Space Innovation (CSI)	☐ Manpower (AF/A1)	☐ Space
☐ AF Cyberspace Operations (AFCO)	☐ Defense Cyber Crime Center (DC3)	☐ Nuclear, non-NC3 (AFNWC)	☐ USAFA
☐ AFOTEC	☐ DT&E	☐ Operational Test Infrastructure (OTI)	☐ Weapons
☐ Air Force Weather (AFWWS)	☐ Finance (SAF/FM)	☐ Rapid Cyber Acquisition (RCA)	☐ Other [see REF: (b)]
☐ Aircraft	☐ Headquarters Air Force (HAF)	☐ Science & Technology (AFRL)	
☐ Civil Engineering (CE)	☐ Industrial Depot Maintenance (IDM)		

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

4. System Operational Status

☐ **Operational** – IT is in production (IOC/FOC)

☐ **Under Development** – IT is in design phase

☐ **Major Modification** – IT is undergoing significant change

5. Proposed Information Technology [Check One from table below]			
Information Systems (IS)	**Platform IT (PIT)**	**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

5. Describe the IT Authorization Boundary

NOTE: This is a text field only; please upload any pictures or diagrams (DoDAF OV-1 and SV-6) to eMASS as artifacts documenting interface requirements

6. Overlays	
6A. *Intelligence Overlay:* Does the IT process, store, or transmit Intelligence, Surveillance, or Reconnaissance (ISR)? Ref: (e)	☐ **Yes** (Intelligence Overlay is required) ☐ **No**
6B. *Cross Domain Solution (CDS) Overlay*: Will you implement, manage, or maintain a CDS? Ref: (d)	☐ **Yes** (CDS Overlay is required) ☐ **No**
6C. Nuclear *Command, Control & Communications (NC3) Overlay:* Does the IT store, process or transmit NC3 data? *NOTE: use of the NC3 Overlay also requires the implementation of the Intel non-NC3* Refs: (n) & (e)	☐ **Yes** (NC3 Overlay is required) ☐ **No**
6D. *Space Platform Overlay:* Is the IT (or subsystem) a space platform (as defined in CNSSI 1253F, Atch 2) and unmanned? Ref: (c)	☐ **Yes** (Space Platform Overlay is required) ☐ **No**
6E. Classified Information Overlay: Does the IT store, process, or transmit classified information? Ref: (f)	☐ **Yes** (Classified Information Overlay is required) ☐ **No**
6F. Mission/Function Specific Overlay: Is your IT required to execute an organizational mission or function-special? (e.g. Financial, Acquisition etc.) Ref: (h)	☐ **Yes** (Specify Overlay) _____ ☐ **No**

7. National Security System (NSS) Designation	
Is this an NSS? NOTE: If the answer to any of the six questions below is "Yes," then the system is an NSS. Ref: (i)	☐ **Yes** ☐ **No**
7A. Does the function, operation, or use of the system involve intelligence activities? Refer to NIST SP 800-59, Appendix A, Paragraph A 1.1 for qualifying criteria.	☐ **Yes** ☐ **No**
7B. Does the function, operation, or use of the system involve cryptologic activities related to national security? Refer to NIST SP 800-59, Appendix A, Paragraph A 1.2 for qualifying criteria.	☐ **Yes** ☐ **No**
7C. Does the function, operation, or use of the system involve military command and control of military forces? Refer to NIST SP 800-59, Appendix A, Paragraph A 1.3 for qualifying criteria.	☐ **Yes** ☐ **No**
7D. Does the function, operation, or use of the system involve equipment that is an integral part of the weapon or weapons system? Refer to NIST SP 800-59, Appendix A, Paragraph A 1.4 for qualifying criteria.	☐ **Yes** ☐ **No**
7E. If the use of the system is not a routine administrative or business application, is the system critical to the direct fulfillment of military or intelligence missions? Refer to NIST SP 800-59, Appendix A, Paragraph A 1.5 for qualifying criteria.	☐ **Yes** ☐ **No**
7F. Does the system store, process, or communicate classified information? Refer to NIST SP 800-59, Appendix A, Paragraph A 1.6 for qualifying criteria.	☐ **Yes** ☐ **No**

8. Cloud	
8A. Is the IT going to be cloud-hosted?	☐ **Yes** ☐ **No** Proceed to Section 9 (Privacy)
8B. Will the IT process classified information (IAW Question 7F)? If YES (IL6) introduce question 8E and 8F (SORN).	☐ **Yes** Proceed to Question 8C ☐ **No** Proceed to Question 8E
8C. Does the IT contain Personally Identifiable Information (PII) other than rolodex information? Ref: (g)	☐ **Yes** (IL6 with Privacy Overlay) ☐ **No** (IL6)
8D. Does your system retrieve information by a unique identifier? (i.e. SSN, Name, DOB, etc.) Refs: (j) & (r)	☐ **Yes** Provide SORN Number, then Proceed to Section 10 _____ ☐ **No** Proceed to Section 10
8E. Does the IT contain Controlled Unclassified Information(CUI), defined in DoDM 5200.01 (Vol. 4) as anything that is not releasable under FOIA or is the CUI limited to Rolodex Information (LOW Personally Identifiable Information) only? Ref: (i) & (s)	☐ **Yes** ☐ **No** (IL2) – Proceed to Section 10 ☐ **Public Facing Website** ☐ **LOW PCIL Determination (**see 8C instructions**)**
8F. Is the IT an NSS System (IAW Section 7) or does it contain information reflected in Ref (i)?	☐ **Yes** ☐ **No Proceed to Question 8I**
8G. Does the IT contain PII other than rolodex information?	☐ **Yes** (IL5 with Privacy Overlay), then Proceed to Question 10 ☐ **No** (IL5)
8H. Does your system retrieve information by a unique identifier? (i.e. SSN, Name, DOB, etc.) Refs: (j) & (r)	☐ **Yes** Provide SORN Number, then Proceed to Section 10 _____ ☐ **No** Proceed to Section 10

8I. Does the IT contain PII other than rolodex information?	☐ **Yes** (IL4 with Privacy Overlay), then Proceed to Question 10 ☐ **No** (IL4)
8H. Does your system retrieve information by a unique identifier? (i.e. SSN, Name, DOB, etc.) Refs: (j) & (r)	☐ **Yes** Provide SORN Number, then Proceed to Section 10 _____ ☐ **No** Proceed to Section 10

9. Privacy

*NOTE: For assistance with completing this section, **please contact your Base Privacy Manager**.*

9A. Will this IT collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nations employed at U.S. military facilities internationally? Ref: (g), Note: (5)	☐ **Yes** ☐ **No** Proceed to Section 10 (See Note 4)
9B. Is the IT an NSS System (IAW Question 7) or does it contain information reflected in Ref (i)?	☐ **Yes** ☐ **No** Proceed to Question 9D
9C. Does it contain PII other than rolodex information? Ref: (g)	☐ **Yes** (Privacy Overlay Required), Proceed to Question 9I ☐ **No** Proceed to Question 9I

9D. What is the context of the CUI, if there is any? (examples: A list of deployed individuals (higher risk due to context), A list of safety meeting attendees (negligable risk due to context))
Ref: (l)

9E. What Type of PII will be contained within or pass through the system? [** Rolodex Information as defined in Ref: (g)]

Could be LOW	**Could be MODERATE**	**MUST BE HIGH**
☐ ** Name (full or partial)	☐ Birth Date	☐ Law Enforcement Information
☐ Employment Information	☐ Place of Birth	☐ Security Information
☐ ** Business Street Address	☐ Race/Ethnicity	☐ Legal Records
☐ ** Business Organization	☐ Financial Information	☐ Protected Health Information (PHI)
☐ ** Business Phone Numbers (includes Fax)	☐ Other ID Number	☐ Medical Information
☐ Official Duty Address	☐ Photo with ephemeris data	☐ Social Security Number (SSN)
☐ Mailing/Home Address	☐ Mother's Middle/Maiden Name	☐ Passport Number
☐ ** Business/Work E-mail Address	☐ Legal Status	
☐ Home/Cell Phone	☐ Emergency Contact	
☐ Mailing/Home Address	☐ DoD ID Number (EDIPI)	
☐ Position/Title	☐ Child Information	
☐ Rank/Grade	☐ Gender/Gender Identification Citizenship	
☐ ** Official Duty Telephone	☐ Drivers License	
☐ Personal E-mail Address		
☐ Photo		

9F. If there is a loss of confidentiality, what type of adverse effect will it have on individuals? Ref: (l)	☐ **Limited**/Minor degradation, damage, loss or harm. ☐ **Serious**/Significant degradation, damage, loss or harm. ☐ **Severe**/Catastrophic degradation, damage, loss or harm.

9G. **Provide detailed example(s) of the potential harm to an individual or organization if the PII were to be compromised**. (Example: the system contains someone's SSN, which could be used to commit identity fraud.)

9H. Determine PII Confidentiality Impact Level Note: Assessment of Impact Level should consider aggregation of all privacy factors (9F-9I) Ref: (l)	☐ Low ☐ Moderate ☐ High
9I. Does your system retrieve information by a personal identifier? (i.e. SSN, Name, DOB, etc.) Refs: (k) & (r)	☐ **Yes** Provide SORN Number ☐ **No** Proceed to Question 10

10. Categorization Information

Categorize the CIA for APPLICABLE Information Types (i.e. Low, Moderate, or High) IAW Ref: (u).

Information Types	Confidentiality	Integrity	Availability	Amplifying Data
FINAL SECURITY CATEGORIZATION				

11. Asset Owner/ Mission Owner/ Government Representatives			
The AF RMF ITCSC was completed by the RMF Team named below. Impact analysis, Security Control Baseline selection, and required overlays have been identified, reviewed and certified.			
Title	**Name**	**Phone (DSN)**	**Organization**
Authorizing Official:*			
AODR:			
Program Manager:*			
SCA:*			
ISSM:*			
Dir. Of Eng./ISSE:			
User Representative:			
Requirements Lead:			
Primary POC:*			

* Mandatory (Minimum Staffing Requirement)

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 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).*
4. *All information systems will need to complete a Privacy Impact Assessment (PIA) in conjunction with an organizational privacy subject matter expert. The PII Confidentiality Impact Level (9H) is a significant contributor to the system categorization and CONFIDENTIALITY level. (Section 10)*
5. *The use of 2 factor authentication (2FA) and Public Key Infrastructure (PKI) in support of Identity, Credential, and Access Management (ICAM) introduces low level PII elements.*

Summary

Describe AF IT: (1)

System Name:	System Acronym:	Version:
ITIPS (if applicable)	DITPR# (if applicable)	eMASS# (if applicable)

Proposed Information Technology (5)

Information Systems	**Platform IT**	**IT Services** ***(Assess Only)***	**IT Products** ***(Assess Only)***
☐ Major Application	☐ PIT Systems	☐ Internal	☐ Software
☐ Enclave	☐ PIT Subsystem(s) *(Assess Only)*	☐ External	☐ Hardware
	☐ PIT Component(s) *(Assess Only)*		☐ Applications

Overlays (6)	**PIA Complete** (9A)	**Operational Status** (4)	**Other**
☐ Security	☐ Yes	☐ Operational	☐ NSS (7)
☐ Space Platform	☐ No	☐ Under Development	
☐ Cross Domain Solution	**Privacy** (9J)	☐ Major Modification	
☐ Intelligence	☐ Low		
☐ Classified	☐ Moderate		
☐ Privacy	☐ High		
☐ Nuclear (NC3)			
☐ Mission Specific Overlay: _____			

Cloud Impact Level (8) or Complete Final IT Categorization (10)

Cloud Impact Level
- ☐ 2
- ☒ 4
- ☒ 5
- ☐ 6
- ☐ N/A

Information Types	**Confidentiality**	**Integrity**	**Availability**
FINAL IT CATEGORIZATION			
JUSTIFICATION			

Approval

AUTHORIZING OFFICIAL:			
Organization:			
Email:			
Phone (Commercial):		Phone (DSN):	
Authorizing Official: (Digital Signature)			
PROGRAM MANAGER:			
Organization:			
Email:			
Phone (Commercial):		Phone (DSN):	
Program Manager / Information System Owner: (Digital Signature)			

INSTRUCTIONS

Aggregation of all data, plus the potential impact and likelihood of a security issue arising from mishandling or misuse of that data, should factor in the assessment of all decisions within the ITCSC.

1. System Identification Information

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

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

Version: Version number of the system

ITIPS ID, DITPR, or eMASS ID numbers may be required if:

- Previous IT registration in ITIPS or eMASS exists.
- You are following the Assess Only Process and integrating a product into a host environment (i.e. the product is a PIT subsystem).
  See Ref: (m) for more information.

2. Technical Description/Purpose

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

- What is the purpose of the IT?
- Is the IT mission essential to the warfighter?
- What are the major hardware/software components of the IT?
- What services are provided by the IT, 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?
- If the IT is undergoing a significant modification, describe the modification and its purpose, otherwise ignore this requirement.

3. 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

4. System Operational Status

Operational - The IT has satisfied program requirements and achieved Initial Operating Capability (IOC) or Full Operating Capability (FOC)

Under Development - The IT is in the design/development phase and has not entered final production/operation.

Major Modification - The IT is undergoing a necessary modification to improve performance and reduce ownership costs, consistent with the limitations prescribed in 10 U.S.C 2244a

5. Describe the IT Authorization Boundary

Provide a narrative that clearly describes the IT 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 is standalone (no external interfaces), then clearly state that in this section.

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) and post it to eMASS as an artifact during or subsequent to initial registration.

6A. Intelligence Overlay

Does the IT process, store, or transmit Intelligence, Surveillance, or Reconnaissance (ISR)?
See Ref: (e) for more information.

6B. Cross Domain Solution Overlay:

Will you implement, manage, or maintain a Cross Domain Solution?
See Ref: (d) for more information.

6C. Nuclear Command, Control & Communications (NC3) Overlay:

Does the IT store, process or transmit NC3 data? Please note that use of the NC3 Overlay also requires the implementation of the Intel non-NC3 Overlay
See Refs: (n) & (e) for more information.

6D. Space Platform Overlay:

Is the IT (or subsystem) a space platform as defined in CNSSI 1253F – Atch 2 and unmanned?
See Ref: (c) for more information

6E. Classified Information Overlay:

Does the IT store, process, or transmit classified information?
See Ref: (f) for more information.

6F. Mission/Function Specific Overlay:

Is your IT required to execute an organizational mission or function-special? (e.g. Financial (FIAR), Acquisition, etc.)
See Ref: (h) for more information

7. National Security System (NSS) Designation

Carefully read and answer questions 7A-7F, checking the Yes or No box on each one. If the answer to any of those six questions is Yes, then the IS is an NSS, (pending review from SAF/CN).
See Ref: (i) for more information.

8A. Cloud Hosted

Is the IT going to be hosted in a cloud environment? If "no," then continue to Question 9.

8B. Classified info through cloud?

If the answers to both 7F and 8A are "Yes," then this will also be checked "Yes" and the Cloud Impact Level will be IL6. If so, proceed to Question 10

8C. Controlled Unclassified Information (CUI)

Does the IT contain CUI, which is defined in DoDM 5200.01 vol. 4 as anything that is not releasable under the Freedom of Information Act (FOIA)?

In order to answer this question NO, the user must answer questions 9D-9G and arrive at a LOW determination for question 9H (Privacy Impact Confidentiality Level)
See Ref: (i) & (s) for more information.

8D. NSS

Has the IS been determined to be an NSS ("Yes" to Question 8), or is it categorized as NSS because of additional factors listed in Ref: (i)?
See Ref: (i) for more information.

8E/G. PII and Rolodex Information

Does the IT contain Personally Identifiable Information (PII) other than information which may meet the parameters of the Rolodex Exception including rosters that contain only business contact information?
See Refs: (g, Paragraph 2.4) for more information.

8F/H. PII information retrieved and SORN

Does the IS retrieve information by a personal identifier? If the IS uses a unique identifier to retrieve information then a System of Records Notice (SORN) is required.
See Ref: (r) for more information.

9: Privacy

For assistance with completing this section, please contact your Base Privacy Manager.

9A. Is IT an NSS system?

If you answered "Yes" to Question 7, then continue. Otherwise, skip to 9E.

9B. PII and Rolodex Information

See instructions under 8E/G, above.

9C: Retrieving Information by a personal identifier

See instructions under 8F/H, above.

9D. CUI / PII Context

Provide context with respect to the CUI or PII stored or transmitted through the IS. For example: Is it a list of deployed individuals (impact would be higher) or a list of individuals who attended a safety meeting (impact would be lower).
See Ref: (l) for more information

9E. PII Types

From the lists provided, identify which PII is applicable to the information in this IS. Information identified as "Rolodex" information is marked with (**) and may be evaluated as Low.
See Ref: (l) for more information

9F. PII Adverse Effect

In 9G you evaluated and made a threat level assessment of the PII in the IS. Further evaluate the PII with respect to the threat to an individuals' data if the information is lost or compromised. 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

9G. Specific Examples of Harm

Describe specific examples of harm that could befall an individual or organization if PII was to be leaked, misused, or otherwise compromised.

9H: PII Confidentiality Impact

IAW 9G-I and Ref: (s), evaluate the Confidentiality Impact Level of the IT. If any factor in 9G-I is considered High, the overall assessment should be High. The aggregation of context, type, and Confidentiality Impact of PII should factor into your consideration.
See Refs: (l) & (s) for more information

10. Categorization Information

In the table, be sure to add main Information Type category above the specific Information Types. For any reduction from the default recommended Security Categorization for each information type, per NIST SP 800-60 Vols 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.

11. Asset Owner/ Mission Owner/ Government Representatives

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 the appropriate approval or authorization documentation before IT testing or operation.

For AF IT, 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) as applicable.

Ensure aggregation of all data, plus the potential impact and likelihood of a security issue arising from mishandling or misuse of that data, is factored in the assessment of all decisions within the ITCSC.

REFERENCES

a) 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.
    - All documentation must be coordinated through the servicing Base and MAJCOM Privacy Manager/Monitor before submission to AF Privacy.
b) AFI 17-101, Risk Management Framework (RMF) for Air Force Information Technology (IT)
c) CNSSI 1253F Atch 2, Space Platform Overlay
d) CNSSI 1253F Atch 3, Cross Domain Solution Overlay
e) CNSSI 1253F Atch 4, Intelligence Overlay
f) CNSSI 1253F Atch 5, Classified Information Overlay
g) CNSSI 1253F Atch 6, Privacy Overlay
h) NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View
i) Additional reference for NSS System Determination
    - 40 U.S.C. § 11103, Applicability to NSS
    - 10 U.S.C. § 130b, Deployment and troop movement
    - 10 U.S.C. § 130e, Military Critical infrastructure
    - Critical Infrastructure Information Act of 2002, Civilian Critical infrastructure
    - 42 U.S.C. § 2162, Unclassified nuclear data
    - 15 U.S.C. §§ 46(f), 57b-2 & 15 U.S.C. §3710a(c), Trade Secrets Act data
    - DoDI 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures
    - 18 U.S.C. § 3771, Crime Victim's Rights Act (DoD implemented by Article 6b, UCMJ—10 U.S.C. § 806b)
    - NIST SP 800-59, Guideline for Identifying an Information System as a National Security System
j) DoD Cloud Computing Security Requirements Guide (Cloud SRG)
k) Privacy Act of 1974
l) NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
m) 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
n) NC3 Overlay: https://rmfks.osd.mil/rmf/SiteResources/References/Reference%20Library/NC3_Overlay.pdf
o) NIST SP 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
p) NIST SP 800-171A: Assessing Security Requirements for Controlled Unclassified Information
q) United States Office of Personnel Management, System of Records Notice (SORN) Guide, dtd April 2010
r) NIST SP 800-60 Volumes 1 & 2: Guide for Mapping Types of Information and Information Systems to Security Categories
s) Treatment of PII within IL2 Commercial Cloud Services for the DoD, 07 AUG 2019