1. Capability Identification Information	
Capability Name:	
Capability Acronym:	
Version:	
DITPR# (if applicable)	
RMF Inventory Tool # (eMASS/XACTA)	

Capability Categorization serves the purpose of assessing and managing the risk associated with information systems. It helps determine the impact levels of potential security breaches, ensuring that appropriate security controls are implemented based on the sensitivity and criticality of the information processed by the capability. This classification is crucial for establishing a robust security posture and aligning security measures with the specific needs and vulnerabilities of the DoD's diverse information systems.

2. Technical Description/Purpose

Describe the purpose of the capability and indicate if the capability is mission-essential to the warfighter:

Describe the MAJOR hardware/software components of the capability:

Describe the services provided by the capability and whether any of the services are publicly accessible (Publicly accessible means does not require authentication to access the information):

Describe how each of the Information Types are, or will be, stored, processed, and/or transmitted by the capability:

3. Capability Owner/Mission Owner/Government Representatives

The CDAO CCS is completed by the Program Manager.

Title	Name	Phone (DSN)	Organization
Information System Security Manager (ISSM):			
Program Manager:			
Authorizing Official Designated Representative (AODR):			
Authorizing Official:			

4. Authorizing Official (Check One) & Authorization Boundary

☐ Advanced Command and Control Accelerator (AC2A)	☐ Directorate for Scaled Capabilities (DSC)	☐ Product Office/Defense Digital Service (PO/DDS)	☐ Chief Information Office (CIO)

☐ CDAO Policy (POL)	☐ Deputy Executive Director (DED)	☐ Chief Technology Office (CTO)	☐ Digital Talent Management (DTM)	☐ Resource Management Office (RMO)

☐ Other (add line to fill in)

5. Capability Operational Status

☐ **Operational** – Has an Authorization from another AO, Seeking CDAO Authorization [ATD: _____; AO: _____]

☐ **Under Development** – New capability, seeking IATT

6. Proposed Capability

6A. Describe the Capability Authorization Boundary: Provide a high-level technical description of the capability diagram. Please also attach a CONOPS and architecture diagram as addendums to this document.

7. Classified Capability Overlays

7A. Intelligence Overlay: Does the capability process, store, or transmit Intelligence, Surveillance, or Reconnaissance (ISR) (as defined in Committee on National Security Systems Instructions (CNSSI) 1253F, Atch 2)?	☐ **Yes** (Intelligence Overlay is required) ☐ **No**
7B. Nuclear Command, Control, and Communications (NC3) Overlay*:* Does the capability store, process or transmit NC3 data? *NOTE: Use of the NC3 Overlay also requires the implementation of the Intelligence Overlay.*	☐ **Yes** (NC3 Overlay is required) ☐ **No**
7C. Classified Information Overlay: Does the information system of interest by intent and design store, process, or transmit classified information?	☐ **Yes** (Classified Information Overlay is required) ☐ **No**
7D. What Intelligence Sensitivity Overlay is needed (e.g., Int A, Int B, Int C)? • Int A – Initial control set to protect the initial information least sensitive. • Int B – Middle control set to protect the information moderately sensitive. • Int C – High control set to protect the information highly sensitive.	
7D. Mission/Function Specific Overlay: Is your capability required to execute an organizational mission or function-special (e.g., Financial, Acquisition etc.)?	☐ **Yes** (Specify Overlay) _____ ☐ **No**
7F. Is the capability going to be cloud-hosted (as defined in Committee on National Security Systems Instructions (CNSSI) 1253F, Atch 2)?	☐ **Yes** (Answer below question) ☐ **No** (Move to next section)
7F (1). Where is it hosted?	

7F (2). What is the Impact Level (e.g., IL-2, IL-4, IL-5, IL-6)?	
7F (3). What FedRamp Baseline is it (e.g., Public/Commercial, Medium, High)?	
8. Cross Domain Solution	
8A. Are you a Cross Domain Solution (CDS) Provider?	☐ **Yes** (CDS Overlay is required) ☐ **No**
8B. Are you using a CDS capability in any way (as defined in Committee on National Security Systems Instructions (CNSSI) 1253F, Atch 2)?	☐ **Yes** (CDS Overlay is required) ☐ **No**
8C. Is the system being developed or used to establish a connection between information systems or networks operating under different security policies that require strict separation of information based on classification, releasability, or sensitivity?	☐ **Yes** (CDS Overlay is required) ☐ **No**
8D. Does the system operate over a range of classification, releasability, or sensitivity levels, where some users are not authorized for all classification, releasability, and sensitivity levels?	☐ **Yes** (Answer the below questions) ☐ **No** (Move to next section)
8D (1). Will the system be used to provide access to different security domains with no requirement to move data between the domains?	☐ **Yes** ☐ **No**
8D (2). Will the system be used to transfer data between different security domains?	☐ **Yes** ☐ **No**
8D (3). Will the system use trusted labeling to associate a classification, releasability, or sensitivity level with objects, allowing users access based upon their security domain and authorized attributes?	☐ **Yes** ☐ **No**
9. Financial Reporting Overlay	
9A. Is this capability processing Financial Reporting Information?	☐ **Yes** (Apply the FISCAM Financial Reporting Overlay) ☐ **No** (Move on to the next section)
9B. Have you assessed the impact of financial reporting overlays on the clarity and transparency of your financial systems and statements?	☐ **Yes** ☐ **No**
9C. Do you have a documented framework for implementing and managing financial reporting overlays?	☐ **Yes** ☐ **No**
9D. Does the information system perform any activity having financial consequences to the Federal Government (i.e., perform a financial / accounting event)?	☐ **Yes** ☐ **No**
9E. Does the system process transactions or store information that directly or indirectly triggers a financial event?	☐ **Yes** ☐ **No**
9F. Does the system collect, process, maintain, transmit, or report data regarding events that impact financial reporting?	☐ **Yes** ☐ **No**

Chief Digital and Artificial Intelligence Office (CDAO)
Risk Management Framework (RMF)
Capability Categorization Summary (CCS)

10. Space Platform Overlay	
10A. Space Platform Overlay: Is the capability (or subsystem) a space platform (as defined in Committee on National Security Systems Instructions (CNSSI) 1253F, Atch 2) and unmanned?	☐ **Yes** (Space Platform Overlay is required) ☐ **No**
10B. Is the system (or subsystem) a space platform as defined in CNSSP No. 12?	☐ **Yes** ☐ **No**
10C. Is the system unmanned?	☐ **Yes** ☐ **No**
10D. Is the system launched and undergoing pre-operational testing or in operation?	☐ **Yes** ☐ **No**

11. National Security System (NSS) Designation	
11A. Does the function, operation, or use of the system involve intelligence activities?	☐ **Yes** ☐ **No**
11B. Does the function, operation, or use of the system involve cryptologic activities related to national security?	☐ **Yes** ☐ **No**
11C. Does the function, operation, or use of the system involve military command and control of military forces?	☐ **Yes** ☐ **No**
11D. Does the function, operation, or use of the system involve equipment that is an integral part of a weapon or weapons system?	☐ **Yes** ☐ **No**
11E. If the system is not used for routine administrative or business applications, is the system critical to the direct fulfillment of military or intelligence missions?	☐ **Yes** ☐ **No**
11F. Does the system store, process, or communicate classified information?	☐ **Yes** ☐ **No**
11G. Does the system process any information whereby the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense or an element of the Intelligence Community?	☐ **Yes** ☐ **No**
11H. Is the system designated as NSS per organizationally defined guidance but does not meet any of the above criteria? If yes, then an appropriate explanation must be provided	☐ **Yes** ☐ **No**

Chief Digital and Artificial Intelligence Office (CDAO)
Risk Management Framework (RMF)
Capability Categorization Summary (CCS)

12. Privacy Overlay	
12A. Does the information system contain PII?	☐ **Yes** (Apply Privacy Overlay) ☐ **No**
12B. Does the Exception of the Business Rolodex Information Apply?	☐ **Yes** ☐ **No**
12C. Is the PII confidentiality impact level low, moderate, or high? Low/Moderate/High	☐ **Yes** (PII Confidentiality Level:_____) ☐ **No**
12D. Is your organization a covered entity or business associate under HIPAA?	☐ **Yes** ☐ **No**
12E. Is the PII in the information system PHI?	☐ **Yes** ☐ **No**
12F. Will this capability 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 (as defined in Committee on National Security Systems Instructions (CNSSI) 1253F, Atch 2)?	☐ **Yes** ☐ **No** (Proceed to Next Section)
12G. Privacy Overlay: Does the capability or application involve the processing of Personally Identifiable Information (PII) (as defined in Committee on National Security Systems Instructions (CNSSI) 1253F, Atch 2)?	☐ **Yes** ☐ **No**
12H. Has the organization started or completed the DD Form 2930 "Privacy Impact Assessment (PIA)?	☐ **Yes** ☐ **No**
12I. Does it contain PII other than name and contact information?	☐ **Yes** (Privacy Overlay Required) ☐ **No**
12J. Is the capability going to be cloud-hosted?	☐ **Yes** ☐ **No**
12K. Does your capability retrieve information by a unique identifier *(i.e., SSN, Name, DOB, etc.)?*	☐ **Yes** (Provide System of Records Notice (SORN) Number) ☐ **No** (Proceed to next section)
12L. Does the capability contain Controlled Unclassified Information (CUI) as defined in DoD Instruction (DoDI) 5200.48, other than Low Impact PII IAW the DoD Memo?	☐ **Yes** ☐ **No** ((IL2) Response requires corresponding entry below.) ☐ **Low Impact PII** ☐ **Public Facing Website**
12M. 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 [negligible risk due to context].)	

Chief Digital and Artificial Intelligence Office (CDAO)
Risk Management Framework (RMF)
Capability Categorization Summary (CCS)

13. Facility Overlay	
13A. Does the system of interest, by intent and design, support control or monitoring of a facility, structure, or linear structure (DoD real property)?	☐ **Yes** ☐ **No**
14. Tactical Deployed Mobile Device Overlay	
14A. Will the information system or one of its components (e.g., CNMF laptops and/or mobile kits) be deployed in foreign theaters of operation, an environment outside of United States Government (USG) control, or in a hazardous location (war zone)?	☐ **Yes** ☐ **No**
14B. Will the information system or one of its components face significant risk of theft, loss or physical compromise while deployed outside of USG control?	☐ **Yes** ☐ **No**
15. Non-U.S. Persons Overlay	
15A. Can an approved DoD enterprise Mission Partner Environment (MPE) for collaboration, such as BICES, be used?	☐ **Yes** ☐ **No**
16. Tactical Radio Overlay	
16A. Is the product going to be used for tactical wireless communication?	☐ **Yes** ☐ **No**
16B. Is the product going to be used for classified tactical wireless communication?	☐ **Yes** ☐ **No**
17. Manufacturing Overlay	
17A. Does the system support DoD manufacturing processes?	☐ **Yes** ☐ **No**

18. Categorization Information

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

Information Types	Confidentiality	Integrity	Availability	Amplifying Data
FINAL SECURITY CATEGORIZATION				

Chief Digital and Artificial Intelligence Office (CDAO)
Risk Management Framework (RMF)
Capability Categorization Summary (CCS)

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

Chief Digital and Artificial Intelligence Office (CDAO)
Risk Management Framework (RMF)
Capability Categorization Summary (CCS)

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 CCS.

1. Capability Identification Information: **(Section 1)**
    a. Capability Name: Enter the capability name (must match Investment Name in IT Investment Portfolio Suite).
    b. Capability Acronym: Use the same acronym as in ITIPS.
    c. Version: Specify the version number.
    d. DITPR#/RMF Inventory Tool#: If applicable, provide identification numbers.

2. Technical Description/Purpose: **(Section 2)**
    a. Describe the capability's purpose, major components, services, and storage/transmission methods for Information Types.
    b. In summary, a technical description delves into the details of how something works, providing a comprehensive view for those with a technical understanding. On the other hand, purpose definition focuses on articulating the underlying reason or goals driving the creation or implementation of a particular technology or capability. Both are essential for effective communication and successful development and deployment of technical solutions.
        i. Technical Description:
            1. Definition: A technical description provides detailed information about the design, structure, features, and functionalities of a capability, product, or process.
            2. Elements: It typically includes specifications, components, architecture, protocols, algorithms, and any other technical details relevant to understanding and implementing the technology.
            3. Purpose: To communicate technical aspects clearly, aiding developers, engineers, or other stakeholders in understanding the intricacies of the subject.
        ii. Purpose Definition:

1. Definition: Purpose definition outlines the reason or objective behind the existence or implementation of a capability, product, or process.
2. Elements: It includes the intended goals, outcomes, or benefits that the entity is expected to achieve.
3. Considerations: The purpose may address business needs, user requirements, or broader organizational objectives.
4. Role in Decision-Making: Clearly defining the purpose helps guide decision-making throughout the development, implementation, and usage phases.

3. IT Authorization Boundary:
    a. The IT Authorization Boundary defines the scope and limits of an information system's security authorization. It delineates the specific components, functions, and data that are covered by the authorization process. This boundary is crucial for assessing and managing security risks as it helps identify what is within the capability's control and what interfaces with external entities.
    b. Key aspects of the IT Authorization Boundary include:
        i. Capability Components: Identifies hardware, software, networks, and personnel that are part of the capability.
        ii. Interfaces: Describes connections and interactions with external capabilities or networks.
        iii. Data Flows: Illustrates the movement of information within the capability and across its boundaries.
        iv. Physical and Logical Boundaries: Encompasses both the tangible and intangible aspects of the capability, including physical locations and logical network configurations.
        v. Capability Security Engineering: Capability security engineering involves designing, implementing, and maintaining secure computer systems. It encompasses risk assessment, threat modeling, and the integration of security measures into the entire development lifecycle. This field aims to protect capabilities from unauthorized access, data breaches, and other security threats.
        vi. Security Controls: Specifies the security measures in place to protect the capability and its components.
    c. Establishing a clear IT Authorization Boundary is essential for effectively managing, assessing, and authorizing the security posture of a capability.

4. Asset Owner/Mission Owner/Government **(Section 3)** Representatives:
    a. Provide contact details for the RMF team, including mandatory roles.

5. Authorizing Official & Authorization Boundary: **(Section 4)**
    a. Choose the relevant Authorizing Official and describe the IT Authorization Boundary.

6. Capability Operational Status: **(Section 5)**
    a. Indicate whether the IT is Operational, Under Development, or undergoing Major Modification.

7. Proposed Information Technology: **(Section 6)**
    a. Define the IT Authorization Boundary in a text field, and upload diagrams to RMF Inventory Tool.

8. Overlays: **(Sections 7 – 17)**
    a. Answer overlay-related questions based on system characteristics. All overlay-related questions have been pulled from eMASS.

9. Privacy: **(Sections 7 – 17)**
    a. Answer questions about PII, CUI, and provide detailed information on the types of PII.
    b. 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 is a significant contributor to the capability categorization and CONFIDENTIALITY level.
    c. Completing a Privacy Impact Assessment (PIA) involves a thorough examination of how a capability, project, or process handles personally identifiable information (PII). Here are key components needed for a comprehensive PIA:
    d. Capability Overview:
        i. Provide a detailed description of the capability or process under assessment.
        ii. Include the purpose, scope, and functionality of the capability.
    e. Data Collection and Use:
        i. Specify the types of PII collected and the purpose for collecting it.
        ii. Describe how the information will be used, including any secondary uses.
    f. Data Sharing:
        i. Identify entities with whom the collected PII may be shared.
        ii. Detail the purposes and mechanisms for sharing, ensuring compliance with privacy laws.
    g. Data Retention and Disposal:
        i. Outline the duration for which PII will be retained.
        ii. Describe secure methods for data disposal since they are no longer needed.
    h. Security Controls:
        i. Detail the security measures in place to protect the confidentiality, integrity, and availability of PII.
        ii. Address encryption, access controls, and other security safeguards.
    i. Privacy Safeguards:
        i. Describe privacy-enhancing features and measures implemented to protect individuals' privacy rights.
        ii. Include mechanisms for obtaining consent if applicable.
    j. Risk Assessment:
        i. Conduct a risk analysis to identify potential privacy risks and assess their likelihood and impact.
        ii. Mitigation strategies should be outlined for identified risks.
    k. Legal and Regulatory Compliance:
        i. Ensure alignment with relevant privacy laws, regulations, and organizational policies.
        ii. Clearly state the legal authority for collecting and processing PII.
    l. Stakeholder Consultation:
        i. Engage with stakeholders, including individuals whose data is being collected, to gather feedback and address concerns.
    m. Documentation and Record-Keeping:
        i. Maintain clear and organized documentation of the PIA process and outcomes.
        ii. Keep records of any changes made based on the assessment.
    n. Review and Update:
        i. Periodically review and update the PIA as the capability evolves or if there are changes in privacy-related factors.
    o. A well-executed Privacy Impact Assessment helps organizations understand and mitigate privacy risks associated with their activities involving PII, fostering transparency and compliance with privacy regulations.

10. System of Records Notice (SORN): **(Sections 7 – 17)**
    a. A SORN is a public notice published in the Federal Register by a federal agency to inform the public about the existence and nature of a system of records.
    b. It details what PII is collected, why it is collected, how it is used, and under what legal authority.
    c. Provides individuals with the right to access and correct their records.
    d. When registering for a SORN, the process typically involves documenting the information system that collects and processes PII. This documentation is crucial for transparency and compliance with privacy laws, such as the Privacy Act in the United States.
    e. Ensure that your organization follows legal requirements, considers privacy best practices, and has appropriate security measures in place when dealing with PII and registering for a SORN.

11. Categorization Information: **(Section 18)**
    a. Reference NIST SP 800-60 vol. 1 and vol. 2; CNSSI 1253 ver. 2; FIPS 199
    b. Categorize Confidentiality, Integrity, Availability for each Information Type.
    c. Categorizing the Confidentiality, Integrity, and

Availability (CIA) of an information system is often done using risk management frameworks. One commonly used framework is the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF). Here's a brief overview:

i. Confidentiality:
   1. Determine the sensitivity of information.
   2. Identify and classify data based on its confidentiality requirements.
   3. Implement access controls, encryption, and other measures to protect sensitive information.

ii. Integrity:
   1. Assess the criticality of data and processes.
   2. Implement mechanisms to ensure data accuracy and reliability.
   3. Use checksums, digital signatures, and access controls to maintain data integrity.

iii. Availability:
   1. Evaluate the importance of capability uptime.
   2. Implement redundancy, failover mechanisms, and disaster recovery plans.
   3. Ensure timely access to resources and services.

iv. These steps involve risk assessments, capability security engineering, security controls, and continuous monitoring to maintain a balance between the three elements. The specific methods may vary based on the organization's needs and the nature of the information system.

12. Final Security Categorization: **(Section 16)**
    a. Reference NIST SP 800-60 vol. 1 and vol. 2; CNSSI 1253 ver. 2; FIPS 199
    b. Capability Name, Acronym, Version, DITPR#/ RMF Inventory Tool#, Proposed IT, Overlays, Privacy Level, Operational Status, NSS Designation, Cloud Impact Level. Program Manager and AO signature blocks for approval.

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 capability.
- All documentation must be coordinated through the CDAO Privacy Manager/Monitor before submission.

b) CNSSI 1253F Atch 2, Space Platform Overlay

c) CNSSI 1253F Atch 3, Cross Domain Solution Overlay

d) CNSSI 1253F Atch 4, Intelligence Overlay

e) CNSSI 1253F Atch 5, Classified Information Overlay

f) CNSSI 1253F Atch 6, Privacy Overlay

g) NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View

- h) 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 Identified.
  - 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

h) DoD Cloud Computing Security Requirements Guide (Cloud SRG)

i) Privacy Act of 1974

j) NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

k) NC3 Overlay: [NC3 Overlay PDF](https://rmfks.osd.mil/rmf/SiteResources/References/Reference%20Library/NC3_Overlay.pdf)

l) NIST SP 800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule

m) NIST SP 800-171A: Assessing Security Requirements for Controlled Unclassified Information

n) United States Office of Personnel Management, System of Records Notice (SORN) Guide, dated 22 April 2010

o) NIST SP 800-60 Volumes 1 & 2: Guide for Mapping Types of Information and Information Systems to Security Categories

p) NIST SP 800-30 Rev. 1: Guide for Conducting Risk Assessments

q) DODI 5200.48: Controlled Unclassified Information (CUI), dated 6 March 2020

r) Department of Defense Chief Information Officer Memorandum, Treatment of Personally Identifiable Information within Information Impact Level 2 Commercial Cloud Services for the Department of Defense, dated 7 August 2019

Appendix A: Privacy Impact Analysis Considerations

A1. Will this capability 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? (as defined in Committee on National Security Systems Instructions (CNSSI) 1253F, Atch 2)	☐ **Yes** ☐ **No** (Proceed to Next Section)
A2. Privacy Overlay: Does the capability or application involve the processing of Personally Identifiable Information (PII)? (as defined in Committee on National Security Systems Instructions (CNSSI) 1253F, Atch 2)	☐ **Yes** ☐ **No**
A3. Has the organization started or completed the DD Form 2930 "Privacy Impact Assessment (PIA)?	☐ **Yes** ☐ **No**
A4. Does it contain PII other than name and contact information?	☐ **Yes** (Privacy Overlay Required) ☐ **No**
A5. Is the capability going to be cloud-hosted?	☐ **Yes** ☐ **No**
A6. Does your capability retrieve information by a unique identifier *(i.e., SSN, Name, DOB, etc.)?*	☐ **Yes** (Provide System of Records Notice (SORN) Number:_____) ☐ **No** Proceed to Next Section
A7. Does the capability contain Controlled Unclassified Information (CUI) as defined in DoD Instruction (DoDI) 5200.48, other than Low Impact PII IAW the DoD Memo?	☐ **Yes** ☐ **No** ((IL2) Response requires corresponding entry below.) ☐ **Low Impact PII** ☐ **Public Facing Website**
A8. 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 [negligible risk due to context])	

A9. What Type of PII will be contained within or pass through the capability?

Could be LOW.	**Could be MODERATE.**	**MUST BE <u>HIGH.</u>**
☐ Business Organization	☐ Birth Date	☐ Law Enforcement Information
☐ Business Phone Numbers (includes Fax)	☐ Child Information	☐ Legal Records
☐ Business Street Address	☐ Citizenship	☐ Medical Information
☐ Business/Work E-mail Address	☐ DoD ID Number (EDIPI)	☐ Passport Number
☐ Employment Information	☐ Driver's License	☐ Protected Health Information (PHI)
☐ Home/Cell Phone	☐ Emergency Contact	☐ Security Information
☐ Mailing/Home Address	☐ Financial Information	☐ Social Security Number (SSN)
☐ Name (full or partial)	☐ Gender/Gender Identification	☐ Disability Information
☐ Official DutyAddress	☐ Legal Status	☐ Education Information
☐ Official Duty Telephone	☐ Mother's Middle/Maiden Name	
	☐ Other ID Number	

Chief Digital and Artificial Intelligence Office (CDAO)
Risk Management Framework (RMF)
Capability Categorization Summary (CCS)

☐ Personal E-mail Address ☐ Photo ☐ Position/Title ☐ Rank/Grade	☐ Photo with ephemeris data ☐ Place of Birth ☐ Race/Ethnicity ☐ Biometrics ☐ Marital Status ☐ Religious Preference	

A10. If there is a loss of Confidentiality, Integrity, and Availability, what type of adverse effect will it have on individuals?	☐ **Limited**/Minor degradation, damage, loss, or harm. ☐ **Serious**/Significant degradation, damage, loss, or harm. ☐ **Severe**/Catastrophic degradation, damage, loss, or harm.
A11. Provide detailed example(s) of the potential harm to an individual or organization if the PII were to be compromised. *(Example: The capability contains someone's SSN, which could be used to commit identity fraud.)*	
A12. Determine PII Confidentiality, Integrity, and Availability, Impact Level *Note: Assessment of Impact Level should consider aggregation of all privacy factors.*	☐ Low ☐ Moderate ☐ High
A13. Does your capability retrieve information by a personal identifier *(i.e., SSN, Name, DOB, etc.)?*	☐ **Yes,** Provide SORN Number: _____ ☐ **No**

Appendix B: Categorization Aide

Data Type	Info Type Title	Confidentiality	Integrity	Availability
~~C.2.4.1~~	~~Contingency Planning Information Type~~	Choose	Moderate	Choose
C.2.4.2	Continuity of Operations Information Type	Moderate	Moderate	Moderate
C.3.5.2	Lifecycle/Change Management Information Type	Low	Modera	Low
C.3.5.5	Information Security Information Type	Low	Moderate	Low
D.1	Defense & National Security	Choose	Choose	Choose
C.3.5.1	System Development	Low	Modera	Low
C.3.5.3	System Maintenance	Low	Modera	Low
C.3.5.4	IT Infrastructure Maintenance	Low	Low	Low
C.3.5.6	Record Retention	Low	Low	Low
C.3.5.7	Information Management	Low	Modera	Low
C.3.5.8	System and Network Monitorin	Moderate	Modera	Low
C.3.5.9	Information Sharing	Choose	Choose	Choose
C.2.8.9	Personal Identity and Authentic	Moderate	Modera	Moderate

- Right side is the default value for CIA, if it is not default, they must identify those appropriately.
- Data Types all out of the NIST SP 800-60 Rev. 2
  - Reference in the text block in section 18.
- Impact and likelihood found in NIST SP 800-30.
  - Reference in the text block in section 18.
- All options for Confidentiality (C), Integrity (I), Availability (A) will only have a determined value of either Low, Moderate, or High.