OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR RESEARCH & ENGINEERING

SUBJECT **SCIENCE AND TECHNOLOGY (S&T) PROTECTION GUIDE**

DATE As of March 31, 2021

REFERENCES See Appendix F

PURPOSE

This document supports requirements outlined in Department of Defense Instruction (DoDI) 5000.83, "Technology and Program Protection to Maintain Technological Advantage," offering guidance and a sample process to assist DoD Components in developing an overall methodology to protect DoD-sponsored S&T programs from unauthorized disclosure. The guidance suggests a process to identify and prioritize threats to, and the vulnerabilities of, (controlled unclassified information (CUI) and classified) critical technology elements and enabling technologies. The guidance also provides example countermeasures and other forms of risk mitigation that DoD Components can implement during the pre-solicitation phase and review continuously thereafter. The Department will implement and update S&T protection as an iterative process, allowing S&T managers to account for program-specific vulnerabilities while maintaining awareness of new and emerging threats to previously identified technology elements.

This document is intended to inform and provide S&T managers, their security support, and technical staffs with example best practices that may be adapted to meet unique organizational needs and program requirements. Appendices B, C, and D provide sample questions that suggest a series of topics that may be covered throughout the S&T protection process. Program[1]-specific requirements will dictate which topics and questions are applicable, and potentially introduce new ones. The questions are intended to facilitate discussions that account for a wide range of threat scenarios and countermeasures, while avoiding simplistic security assessments more commonly associated with checklist requirements.

APPLICABILITY

This process applies to the Office of the Secretary of Defense (OSD), the Military Departments (MILDEPs), the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, and the Defense Agencies (collectively known as DoD Components).

[1] Programs, studies, and projects will be collectively referred to as "Programs" in this guide.

APPROACH

DoD Components have a responsibility to establish policies, plans, and procedures to assess the level of acceptable risk of adversarial exploitation and technology compromise. The approach detailed in this guide includes a fundamental research review to identify fundamental research scope and a risk assessment to determine the degree of exposure and the impact to national security. The results of this analysis should be documented in writing and approved by a DoD Component-specified "Risk Owner[2]" prior to issuance of solicitations. If the process reveals elements of information requiring protection or risk factors requiring mitigation, these factors and their associated countermeasures should be documented in an S&T Protection Plan[3], which the organization should review at least annually. **Appendix A,** "S&T Risk Management Framework," depicts how each of the steps detailed below inform and support risk management functions throughout a program's lifecycle. Please note, the steps provided below may be tailored to meet organizational and program needs. A program may not require the application of every step, depending on the scope of associated research and the risk tolerance of the organization.

1. Fundamental Research Review. In this document, we utilize the definition of Fundamental Research (see Appendix G.2.) provided in Reference (u). The fundamental research review represents the first step in the S&T risk management framework, utilizing a defined and repeatable process to certify the scope of the research to be conducted. The process should include a documented decision on fundamental research scope early in the process. The term "documented" is defined as formally recording the rationale and factors considered when the decision was made. The term "early" is defined as when the solicitation or program scope begins to solidify, but prior to discussing the program content in the public domain. This decision should be made with input from program management and security staff based on information derived from the intelligence, counterintelligence (CI), and law enforcement communities.

Appendix B, "Fundamental Research Review Template," provides an example fundamental research review that should assist in developing the scope of research activities to be in compliance with the Under Secretary of Defense (Acquisition, Technology, and Logistics) Memorandum, "Fundamental Research," May 24, 2010 and for determining the most appropriate award vehicle to use. If all questions in Appendix B are TRUE, then the research can safely be considered fundamental and awarded via an assistance agreement (i.e., grant or cooperative agreement). If any of the questions are FALSE, the S&T manager should coordinate with security staffs, CI representatives, and export control representatives to complete the technology element identification questions. Government S&T managers and security staff should use the fundamental research review when developing the solicitation and when reviewing proposals prior to award. Government S&T managers and college, university, and laboratory researchers

[2] It is recommended that the risk owner for a program be an official at a level of authority above the S&T Manager.
[3] The S&T Protection Plan Template is provided as an accompanying document to this guide and serves as an example iterative record of risk management to be referenced and reviewed over a program's lifecycle.

should also use these questions to monitor the execution of research. When stakeholders appropriately scope contracted fundamental research, the risk to national security is negligible.

2. Technology Element Identification Questions. Should the fundamental research review determine that a program does not warrant categorization[4] as fundamental research, a series of questions should be reviewed to identify key elements of program information that may require protection. Information elements that require protection include critical technology elements, enabling technologies related to the program, Controlled Unclassified Information (CUI)[5], and classified information. Critical technology elements and enabling technologies may be identified by the following:

- DoD Modernization Priorities
- List of Critical Programs and Technologies for Prioritized Protection
- Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) Technology Area Protection Plans (TAPPs)
- Service/Agency Priorities
- Other Priorities, as appropriate

Section One of **Appendix C**, "Sample Technology Element Identification Questions & Upfront Research Risk Assessment," provides an example series of questions. The answers to these questions may later be captured in Section Two of the S&T Protection Plan, serving as a means to document and update information elements requiring protection over the program's lifecycle. If stakeholders determine that the program contains information elements requiring protection, an upfront risk assessment is required to determine the need for a formal S&T Protection Plan.

3. Upfront Research Risk Assessment. After utilizing the technology element identification questions to identify information elements requiring protection, stakeholders should conduct an upfront research risk assessment to determine the risk associated with the unauthorized disclosure of that information. In supporting the requirements for an initial risk assessment as outlined in DoDI 5000.83, this assessment should account for the impacts of unauthorized disclosure on the program as a whole, as well as potential impacts to related programs, national security, and the economic prosperity of the United States. Additionally, the assessment should list currently identified threats and vulnerabilities associated with the information elements previously identified, regardless of program-specific risks or more generalized and widely applicable risks. Whenever possible, the assessment should identify programs that contain technology elements or areas that are tied to the interests of specific state actors. Finally, S&T managers should use the upfront research risk assessment to formulate a means to maintain awareness of emerging threats and vulnerabilities, and plan for the integration of that information into the risk assessment process over the program's lifecycle. Sections Two

[4] See DoDI 5000.83 regarding requirements for categorization in research.
[5] See Reference (d) for more information.

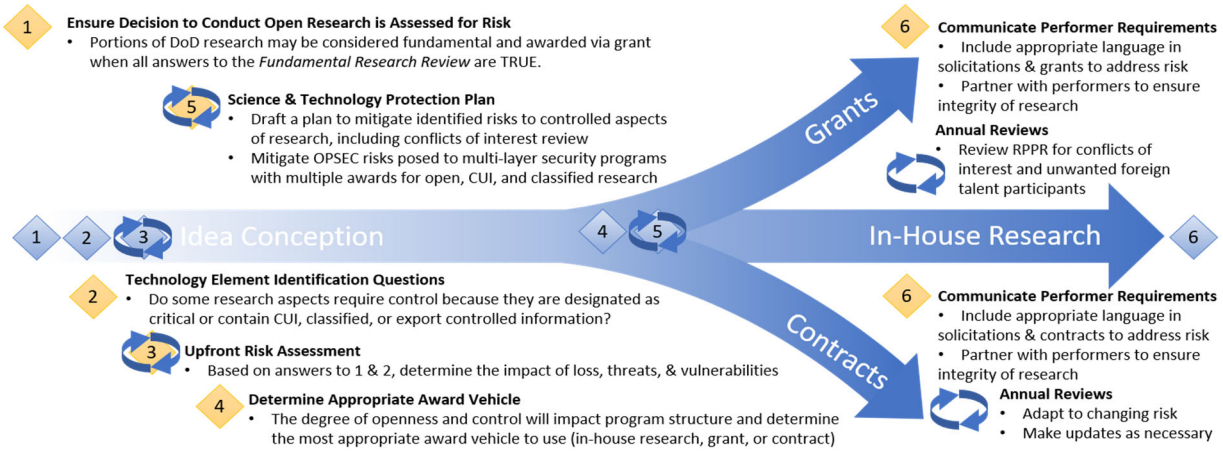
and Three of **Appendix C** provide an upfront research risk assessment sample, while **Appendix E,** "Risk Assessment Definitions," establishes a series of accompanying risk definitions. These questions may later be incorporated as sections two and three of the formal S&T Protection Plan, enabling S&T managers to reassess risk factors over the program's lifecycle.

4. S&T Protection Plan. Following the risk assessment, the risk owner will determine whether a formal S&T Protection Plan is required to develop countermeasures and address unacceptable risk factors. As identified in DoDI 5000.83, the S&T Protection Plan must document, at a minimum, (1) critical technology elements and enabling technologies, (2) threats to, and vulnerabilities, of these items, and (3) selected countermeasures to mitigate associated risks. The document is intended to be iterative, allowing S&T managers to account for changes to a program that may result in the introduction of previously unidentified risks (e.g. the rotation of personnel with program access, new and emerging threats, required exceptions for testing and evaluation, etc.). The example S&T Protection Plan provided consists of the following five sections:

1. Responsible points of contact (POCs) for the program: Serves to identify key government and contractor personnel that will either be responsible for, or have access to, the program. Additionally serves to document the completion of any required trainings.
2. Technology element identification and risk assessment: This section is informed by the answers identified in both the technology element identification questions and upfront research risk assessment, and allows S&T managers to assess previously unidentified information elements that may be encountered over the program's lifecycle.
3. Identified threats and vulnerabilities: This section is similarly informed by the answers identified in the upfront research risk assessment and serves to account for previously unidentified threats over the program's lifecycle.
4. Countermeasures and risk mitigation plan: Tailored countermeasures are identified as they relate to the information elements and threats identified in sections Two and Three, respectively. This section represents the bulk of the protection plan and acts as a risk mitigation framework for S&T managers. While Section One of **Appendix D,** "Sample Countermeasures and Response Questions," lists a series of example questions to facilitate the development of countermeasures, additional tailoring may be necessary to meet program-specific requirements.
5. Response, recovery, and support: Establishes a method for reporting unauthorized disclosures, identifying appropriate CI, security, and law enforcement points of contact. Additionally, this section should discuss policies for remediation to ensure that appropriate action is taken to address violations of disclosure requirements. Section Two of **Appendix D** lists a series of example questions that S&T managers may use to facilitate a response and recovery plan, although additional tailoring may be necessary to meet program-specific requirements.

APPENDIX A: S&T RISK MANAGEMENT FRAMEWORK

Purpose: The following graphic depicts a general process flow for conducting S&T risk management. Each step in this process is intended to be tailored to meet organizational needs and program requirements based on a detailed risk assessment. Depending on the scope of the research, the program may not require the application of every step as depicted below. For example, if all answers to the Fundamental Research Review are TRUE, the process flow may proceed directly from Step 1 to Step 6 (grants). These guidelines support a risk management process that is iterative and adaptable to changing risk over a program's lifecycle.



1	Fundamental Research Review	Assess research to determine if parts can be done openly without restriction
2	Tech Element ID Questions	Identify aspects designated as critical, export controlled, CUI, or classified
3	Upfront Risk Assessment	Determine the criticality of each aspect and identify threats and vulnerabilities
4	Determine Award Vehicle	Depending on the openness of the research and the necessary controls
5	Draft S&T Protection Plan	Draft a plan to mitigate identified risks to controlled aspects of research
6	Communicate Requirements	Include appropriate protection language in solicitations, grants, & agreements

APPENDIX B: FUNDAMENTAL RESEARCH REVIEW TEMPLATE

Purpose: The Fundamental Research Review is conducted to determine whether a program contains **elements** that may be pursued openly without restriction or may require additional protection considerations. This review provides an ideal starting point for identifying and documenting a program's various technology elements, which later serves to inform the S&T Protection Plan, Security Classification Guide, and other program requirements.

Intended User/Audience: S&T Managers in coordination with security staffs and CI representatives.

1. FUNDAMENTAL RESEARCH REVIEW QUESTIONS

The scope and results of the solicitation/contract is likely fundamental research when all responses to the following statements are TRUE:

	QUESTION **The scope and results of the contract, grant, agreement, or other transaction authority:**	**TRUE OR FALSE**
1.	Would ordinarily be published and shared broadly within the scientific community without restrictions.	
2.	Will NOT have a negative impact on national security when disclosed in the public domain, or combined with other available public domain information.	
3.	Is NOT covered in the International Traffic in Arms Regulations (ITAR) (i.e., enumerated on the U.S. Munitions List) or listed on the Export Administration Regulations' Commerce Control List (CCL) (e.g., listed with an Export Control Classification Number (ECCN)).	
4.	Will NOT contain proprietary research from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons.	
5.	Do NOT require classification consistent with EO 13526, "Classified National Security Information."	
6.	Do NOT involve disclosing performance characteristics of military systems or national intelligence or unique development, manufacturing, assembly, testing, operation, maintenance, or repair processes that are critical to defense.	
7.	Do NOT require access to controlled unclassified or classified information to support the conduct of the research.	

2. TECHNOLOGY ELEMENT IDENTIFICATION

Identify and list technology elements contained within the program, characterized by protection requirements:

Open Research Elements*	Controlled Unclassified Information (CUI) Elements	Classified Information Elements
1. 2. 3. 4. 5.	1. 2. 3. 4. 5.	1. 2. 3. 4. 5.

*Only research elements for which all answers to the Fundamental Research Review Questions are TRUE may be considered open research elements. While open research elements do not require documented protections, the recommendation to document them here serves to track those elements over a program's lifecycle.

APPENDIX C: SAMPLE TECHNOLOGY ELEMENT IDENTIFICATION QUESTIONS & UPFRONT RESEARCH RISK ASSESSMENT

Purpose: The Technology Element Identification Questions are intended to identify key elements of program information that may require protection, such as critical technology elements, enabling technologies related to the program, Controlled Unclassified Information (CUI), and classified information. These questions (1. Technology Element Identification) may later be incorporated in Section Two of the S&T Protection Plan.

The Upfront Research Risk Assessment is intended to aid in determining the risk associated with the unauthorized disclosure of key elements of program information identified in the Technology Element Identification Questions. These questions (2. Assessed Impact of Loss, Theft, or Compromise of Information and 3. Identified Threats and Vulnerabilities) may later be included as Sections Two and Three of the S&T Protection Plan, respectively.

Section Four (4. Recommendation and Justification Template) provides an example template for documenting the risk owner's decision regarding acceptable levels of risk, following the completion of the Upfront Research Risk Assessment. The presence of unacceptable risk factors will require the drafting of a formal S&T Protection Plan, applying countermeasures, and formulating response, recovery, and support processes.

Intended User/Audience: S&T Managers in coordination with security staffs, CI Representatives, and Export Control Representatives.

1. TECHNOLOGY ELEMENT IDENTIFICATION

1.1. Does this program contain any open research elements that do not require additional protection considerations?
1.2. Does this program contain critical technology elements or enabling technologies as identified by:
  1.2.1. DoD Modernization Priorities
  1.2.2. List of Critical Programs and Technologies for Prioritized Protection
  1.2.3. OUSD(R&E) Technology Area Protection Plans (TAPPs)
  1.2.4. Service/Agency Priorities
  1.2.5. Other Applicable Priorities
1.3. Do identified critical technology elements or enabling technologies have applications across multiple domains or priorities? (*Note: The presence of this information necessitates responses in Sections 1.7.1 and 1.7.2 of Appendix D*)
1.4. Does this program contain export control information? (See References (a), (n), and (o) for Applicable Authorities) (*Note: The presence of export control information necessitates responses in Sections 2.2.1, and 2.2.2, as well as Sections 1.3.4, 1.3.5, 1.3.6, 1.3.7 and 1.6.2 of Appendix D*)

1.5. Does this program contain Controlled Unclassified Information (CUI) e.g. Controlled Technical Information (CTI)? (See References (d) and (p) for Applicable Authorities) (*Note: The presence of CUI necessitates responses in Sections 2.3.1, 2.3.2, and 3.2.2, as well as Sections 1.3.2, 1.3.5, 1.3.6, 1.3.7, and 1.4.5 of Appendix D*)

1.6. Does this program contain classified information? (*Note: The presence of classified information necessitates responses in Sections 2.4.1, 2.4.2, and 3.2.3*)

2. ASSESSED IMPACT OF LOSS, THEFT, OR COMPROMISE OF INFORMATION

2.1. Critical Technology Elements

- 2.1.1. What is the impact of loss, theft, or compromise of information related to critical technology elements or enabling technologies? (*Note: Utilize a series of risk definitions such as those provided in Appendix E)*
- 2.1.2. Describe the impact of loss, theft, or compromise of information related to each identified technology element on the program as a whole, as well as potential impact to related programs.
- 2.1.3. If the program achieves its proposed goals, what would be the impact to the U.S. warfighting capability if the technology is released, compromised, or stolen prior to an official decision to classify or release the program's results?

2.2. Export Control Information (See References (a), (n), and (o) for Applicable Authorities) (*Note: Given the potential for overlap, this section is intended to cover elements of export control information not already sufficiently captured in Section 2.1)*

- 2.2.1. What is the impact of loss, theft, or compromise of export control information?
- 2.2.2. Describe the impact of loss, theft, or compromise of export control information on the program as a whole, as well as potential impact to related programs.

2.3. Controlled Unclassified Information (CUI) (See References (d) and (p) for Applicable Authorities)

- 2.3.1. What is the impact of the unauthorized disclosure of CUI, to include CTI?
- 2.3.2. Describe the impact of the unauthorized disclosure of CUI elements on the program as a whole, as well as potential impact to related programs.

3. IDENTIFIED THREATS AND VULNERABILITIES

3.1. Are there threats (e.g., adversary collection methods) specific to or assessed as more likely given the program's content or intent?

3.2. Does the program include a technology element or area tied to the interests of specific state actors?

- 3.2.1. Would the loss, theft, or compromise of information related to critical technology elements or enabling technologies likely result in foreign adversaries filling critical technology gaps?
- 3.2.2. Would the unauthorized disclosure of CUI elements likely result in foreign adversaries filling critical technology gaps?

3.2.3. Would the loss, theft, or compromise of classified information likely result in foreign adversaries filling critical technology gaps?

4. RECOMMENDATION AND JUSTIFICATION TEMPLATE

RECOMMENDATION.

The [Risk Owner] has categorized [and classified, if necessary] the [Program Name] program as a [Fundamental Research, Controlled Unclassified Information, Collateral, SAP, SCI, or combination thereof] program and determined that the regulatory protections associated with that categorization/classification [are or are not] sufficient to mitigate the security risks to the program. Therefore, it is recommended that an S&T Protection Plan [is or is not] required to further document risk factors and develop applicable countermeasures.

JUSTIFICATION.

[Provide a summary overview of the Upfront Research Risk Assessment that supports the decision to move forward with or without an S&T Protection Plan.]

APPENDIX D: SAMPLE COUNTERMEASURES AND RESPONSE QUESTIONS

Purpose: The following questions are intended to guide the development of a risk mitigation and response plan for previously identified key elements of program information. The first group of questions (1. Countermeasures and Risk Mitigation Plan) serves as Section Four of the S&T Protection Plan, while the second group of questions (2. Response, Recovery, and Support) serves as the fifth and final section.

Intended User/Audience: S&T Managers in coordination with security staffs, CI Representatives, Law Enforcement, and Export Control Representatives.

1. COUNTERMEASURES AND RISK MITIGATION PLAN

1.1. Personnel

1.1.1. What process is being utilized to grant and document access for personnel that will actively work on the program? (See References (t), (v), (w) and (ee) for Applicable Authorities)

1.1.2. What processes will be utilized to identify and resolve reported/discovered conflicts of interest or commitment (e.g., use of Standard Form 424)? (See References (b), (r), (s), (aa) and (ee) for Applicable Authorities) (*Note: Most universities maintain applicable internal policies*)

1.1.3. What process is being utilized to track and maintain accountability for foreign visits? (*Note: No associated DoD policy applicable to academic institutions conducting DoD-sponsored research*)

1.1.4. What process is being utilized to track and maintain accountability for foreign travel of personnel? (See Reference (aa) for Applicable Authorities)

1.2. Foreign Involvement

1.2.1. Describe any planned, existing, or anticipated international cooperative development activities related to the program.

1.2.2. How are planned, existing, and anticipated foreign vendor engagements and procurements of critical products and services reviewed for risk (e.g. malicious software, hardware, deemed exports, unauthorized disclosure, etc.)? How are such engagements documented?

1.3. Training

1.3.1. Describe the training conducted to inform personnel about safeguarding critical technology elements. (See Reference (c) for Applicable Authorities)

1.3.2. Describe the training conducted to inform personnel about safeguarding CUI, to include CTI. (See References (d) and (p) for Applicable Authorities)

1.3.3. Describe the training conducted to inform personnel regarding insider threats as they relate to the program. (See References (w), (x), (y), (bb), (cc) and (dd) for Applicable Authorities)

1.3.4. Describe the training conducted to inform personnel regarding export control policies, if applicable. (See References (a), (n), and (o) for Applicable Authorities)
1.3.5. What resources were used to develop each training program?
1.3.6. How often is each training conducted?
1.3.7. How is the completion of training tracked?

1.4. Information Technology (See References (i), (m), (x), and (y) for Applicable Authorities)
1.4.1. Are systems NIST SP 800-171 compliant?
1.4.2. Identify non-compliant systems, actions taken to mitigate risk and seek compliance, identify timelines for compliance.
1.4.3. How will IT systems be transported away from the work site? What restrictions are in place regarding the transport of IT systems?
1.4.4. What policies are in place regarding the use of personal electronic devices in the vicinity of work sites?
1.4.5. What attribution methods are utilized to ensure the accountability and integrity of research data and CUI? (See Reference (z) for Applicable Authorities)

1.5. Physical Security (See References (d) and (p) for Applicable Authorities)
1.5.1. What measures are in place to prevent physical access to information and systems by unauthorized personnel?
1.5.2. How will physical documents and electronic media be stored? Container type? How is access granted/controlled?
1.5.3. How will physical documents be destroyed?
1.5.4. How will documents, materials, technology, and systems be transported or shipped?

1.6. Program-Specific Countermeasures
1.6.1. Will specific technology elements require unique protections not applicable to the program as a whole?
1.6.2. How will required International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR) protection procedures be documented and applied to the program? (See References (a), (n), and (o) for Applicable Authorities)

1.7. Horizontal Protection
1.7.1. What process is in place for protecting critical technology elements or enabling technologies that have applications across multiple domains or priorities?
1.7.2. Have external points of contact been identified for protection coordination?

1.8. Emerging Threats and Vulnerabilities
1.8.1. What plan is in place to maintain awareness of emerging threats and vulnerabilities?
1.8.2. How will emerging threats and vulnerabilities be integrated into the existing plan?

1.9. Test Planning, Experimentation, and Evaluation Outside of Protected Environments
1.9.1. Does any portion of the program involve elements of testing or evaluation that require an exception to outlined protection requirements?

1.9.2. If yes, describe the process that will be utilized to mitigate previously identified threats or vulnerabilities under these conditions.

1.10. Technology Transition Plan

1.10.1. Is it anticipated that technology elements will be transitioned as component or sub-component technologies? As a complete system?

1.10.2. List any transition partners that have been identified for this program (Program Executive Offices (PEOs), Combat Capability Development Centers (CCDCs), industry partners, etc.).

1.10.3. Are there any security-relevant transition/mission partner requirements that the program needs to incorporate into a plan (security classification guidance, anti-tamper requirements, OPSEC considerations or association concerns, etc.)?

1.10.4. Is there a signed Transition Agreement (TA), Technology Transfer Agreement (TTA), Memorandum of Agreement (MOA), or Memorandum of Understanding (MOU) governing the transition agreement between the S&T organization and the transition/mission partner? If so, are critical risks and security-relevant requirements specified in said agreement? If a signed agreement does not exist, how will security risks and requirements be transitioned to the mission owner, and how will their buy-in to the transition process be documented?

1.10.5. What intellectual property (e.g., technical data and computer software deliverables, patented technologies and associated license rights, etc.) is required to support acquisition and sustain the product lifecycle for the recipient?

1.10.6. What are the intellectual property rights pertaining to the government?

1.10.7. What type of data rights are required (unlimited, government purpose, restricted, or limited)?

1.11. Published Work and Communications Plan (See References (d), (e), (j), and (k) for Applicable Authorities)

1.11.1. What guidelines are in place to protect critical technology elements from disclosure through publishing or communications with the public?

1.11.2. Is a public affairs plan in place to communicate program details while limiting unauthorized disclosure?

1.11.3. What process for pre-publication review is in place?

2. **RESPONSE, RECOVERY, AND SUPPORT**

2.1. Reporting Requirements

2.1.1. Which Personnel Security (PERSEC) Managers, Information Security (INFOSEC) Managers, Foreign Disclosure Representatives, and Export Control Representatives have been identified as POCs for response coordination?

2.1.2. What reporting instructions are being utilized to inform counterintelligence, security, and law enforcement POCs of breaches of protection policies? (See References (f), (g), (h), and (l) for Applicable Authorities)

2.2. Remediation

2.2.1. What policies are in place to ensure appropriate action is taken for violation of disclosure requirements?
2.2.2. What policies and procedures are in place to respond to intentional penetrations of cyber and physical security systems?

APPENDIX E: RISK ASSESSMENT DEFINITIONS

1. ASSESSED IMPACT OF LOSS, THEFT, OR COMPROMISE OF INFORMATION

Select one answer below for each critical component (i.e., critical technology elements, enabling technologies, etc.) that best describes the advantage you believe the adversary would receive. Also consider the effect it would have on the U.S. should the information or technology be subject to an unauthorized technology transfer disclosure:

CRITICAL. Unauthorized disclosure of research information or technology could provide an adversary key information to bypass significant research and development programs; cause significant degradation in mission effectiveness; shorten the lead-time advantage of the program; significantly alter program direction; or enable the adversary to copy, clone, counter, defeat, and/or reverse engineer the technology or capability.

HIGH. Unauthorized disclosure of research information or technology could provide an adversary information to refine research and development programs, may degrade mission effectiveness, alter program direction, or cue an adversary to target the program in order to copy, clone, counter, and defeat technologies/efforts. An industry performer's lead-time advantage, competitiveness, economic market, and mission standing for this technology space could be put at risk.

MEDIUM. Unauthorized disclosure of research information or technology could provide an adversary adequate knowledge to focus a research or development program on a similar path or with a specific technical approach that could reduce the lead-time advantage. Industry stakeholders in the technology market space could face increased targeting.

LOW. Unauthorized disclosure of research information or technology does little to change the capability or program direction. It may provide an adversary minimal knowledge about the program and its intent. However, that knowledge would be easy to obtain with little effort or does not require extensive expertise.

NONE. Unauthorized disclosure of research information or technology could not be used in any way to reduce the capability or alter the research direction. The information is accessible from the public domain or is available for purchase.

APPENDIX F: REFERENCES

(a) DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," March 27, 2014, incorporating Change 1, July 31, 2017

(b) DoD Instruction 3210.7, "Research Integrity and Misconduct," May 14, 2004, incorporating Change 1, October 15, 2018

(c) DoD Instruction 5000.83, "Technology and Program Protection to Maintain Technological Advantage," July 20, 2020

(d) DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 06, 2020

(e) DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014, incorporating Change 1, April 14, 2017

(f) DoD Instruction 5240.04, "Counterintelligence (CI) Investigations," April 1, 2016, incorporating Change 1, April 26, 2018

(g) DoD Instruction 5240.19, "Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP)," January 31, 2014, incorporating Change 1, August 17, 2017

(h) DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011

(i) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, incorporating Change 1, October 7, 2019

(j) DoD Directive 5230.09 "Clearance of DoD Info for Public Release," January 25, 2019

(k) DoD Directive 5230.25 "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984, incorporating Change 2, October 15, 2018

(l) DoD Directive O-5240.02 "Counterintelligence (CI)," March 17, 2015, incorporating Change 1, May 16, 2018

(m) Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," December 31, 2019

(n) 15 Code of Federal Regulation (CFR), Chapter VII, Subchapter C, "Export Administration Regulations" January 01, 2012

(o) 22 Code of Federal Regulation (CFR), Chapter I (DoS), Subchapter M, "International Traffic in Arms Regulations" April 01, 2011

(p) 32 Code of Federal Regulation (CFR) 2002, "Controlled Unclassified Information (CUI)," September 14, 2016

(q) 32 Code of Federal Regulation (CFR) 236, “Department of Defense (DoD) – Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance (CS/IA) Activities,” July 01, 2013

(r) Federal Acquisition Regulation (FAR) 52.203-16, “Preventing Personal Conflicts of Interest,” December 02, 2011

(s) Federal Register, Volume 65, page 76262, December 6, 2000, "Federal Policy on Research Misconduct," current edition

(t) Sections 1286, “National Defense Authorization Act for Fiscal Year 2019, “Initiative to Support Protection of National Security Academic Researchers from Undue Influence and other Security Threats,” August 13, 2018

(u) Under Secretary of Defense (Acquisition, Technology, and Logistics) Memorandum, “Fundamental Research,” May 24, 2010

(v) Under Secretary of Defense (Research & Engineering) Memorandum, “Actions for the Protection of Intellectual Property, Controlled Information, Key Personnel, and Critical Technologies,” March 20, 2019

(w) Committee on National Security Systems Directive (CNSSD) 504, “Directive on Protecting National Security Systems from Insider Threat,” September 15, 2016

(x) National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-53 Rev. 5 (Draft), “Security and Privacy Controls for Information Systems and Organizations,” March 16, 2020

(y) National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171 Rev. 2, “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,” February 21, 2020

(z) National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171b (Draft) “Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets,” June, 2019

(aa) National Security Presidential Memorandum (NSPM) 33, “United States Government-Supported Research and Development National Security Policy,” January 14, 2021

(bb) Executive Order 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,” October 07, 2011

(cc) White House Memorandum, “National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs,” November 21, 2012

(dd) White House Memorandum, “Compliance with President’s Insider Threat Policy,” July 19, 2013

(ee) Higher Education Act of 1965, November 8, 1965

APPENDIX G: GLOSSARY

1. ABBREVIATIONS AND ACRONYMS

CI	Counterintelligence
CFR	Code of Federal Regulations
CoC	Conflict of Commitment
CoI	Conflict of Interest
CTI	Controlled Technical Information
CUI	Controlled Unclassified Information
DFARS	Defense Federal Acquisition Regulation Supplement
DIB	Defense Industrial Base
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
EAR	Export Administration Regulations
ITAR	International Traffic in Arms Regulations
OUSD(R&E)	Office of the Under Secretary of Defense for Research and Engineering
R&D	Research and Development
SCG	Security Classification Guide
SCI	Sensitive Compartmented Information
S&T	Science and Technology
TAPP	Technology Area Protection Plan
USG	United States Government

2. **DEFINITIONS**

Unless otherwise noted, these terms and their definitions are for the purposes of this document.

Controlled Technical Information (CTI). Technical information with military or space application that is subject to controls on its access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

Controlled Unclassified Information (CUI). The term used to collectively describe any unclassified information that is determined to be exempt from public disclosure in accordance with national laws, policies, and regulations, including critical technology subject to export control to which access or distribution limitations have been applied.

Conflict of Commitment (CoC). A conflict of commitment is a situation in which an individual accepts or incurs conflicting obligations between or among multiple employers or other entities. Many institutional policies define conflicts of commitment as conflicting commitments of time and effort, including obligations to dedicate time in excess of institutional or funding agency policies or commitments. Other types of conflicting obligations, including obligations to improperly share information with, or withhold information from, an employer or funding agency, can also threaten research security and integrity, and are an element of a broader concept of conflicts of commitment.

Conflict of Interest (CoI). A conflict of interest is a situation in which an individual, or the individual's spouse or dependent children, has a financial interest or financial relationship that could directly and significantly affect the design, conduct, reporting, or funding of research.

Critical Technology. Sensitive technical data, concepts, hardware, software, processes, know-how, design details, scientific information, research results, and capability elements that are essential to (or reveal) the design, research, development, production, operation, application, performance, or maintenance of an article, capability, or service that significantly contributes to a current or future U.S. technological, competitive, or lethal advantage over a foreign adversary capability, whose acquisition by potential adversaries would prove detrimental to the national security of the United States.

Critical Technology Element. A new or novel technology that a platform or system depends on to achieve successful development or production or to successfully meet a system operational threshold requirement. Technology Readiness Levels (TRL) are a method of estimating the technology maturity of a Critical Technology Element.

Emerging Threat. A threat that may be newly recognized; may have been recognized before but may potentially affect a new or different population, industry, or geographic area than previously affected; or may be an existing threat that has developed new attributes.

Fundamental Research. Basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons. See Reference (u) for further information.

Technology Area Protection Plan (TAPP). An OSD document that adapts and applies principles of program protection planning to each S&T Modernization Priority Area. TAPPs provide a decomposition of each modernization area into its critical sub-elements and enabling technologies, define technical thresholds that require protection, offer communication guidance, and suggest Department- and program-level risk mitigations to help consistently protect emerging and existing DoD S&T investments at conception and throughout the program lifecycle. TAPP appendices include known contracts and grants; DoD programs and research programs; classification guides; international agreements; vendors, research centers, and companies relevant to the Modernization Priority Area.

Unauthorized Disclosure. An unapproved communication or physical transfer of non-public information, controlled unclassified information, or classified information, to a recipient not permitted to receive such information.