Report No. DODIG-2022-113

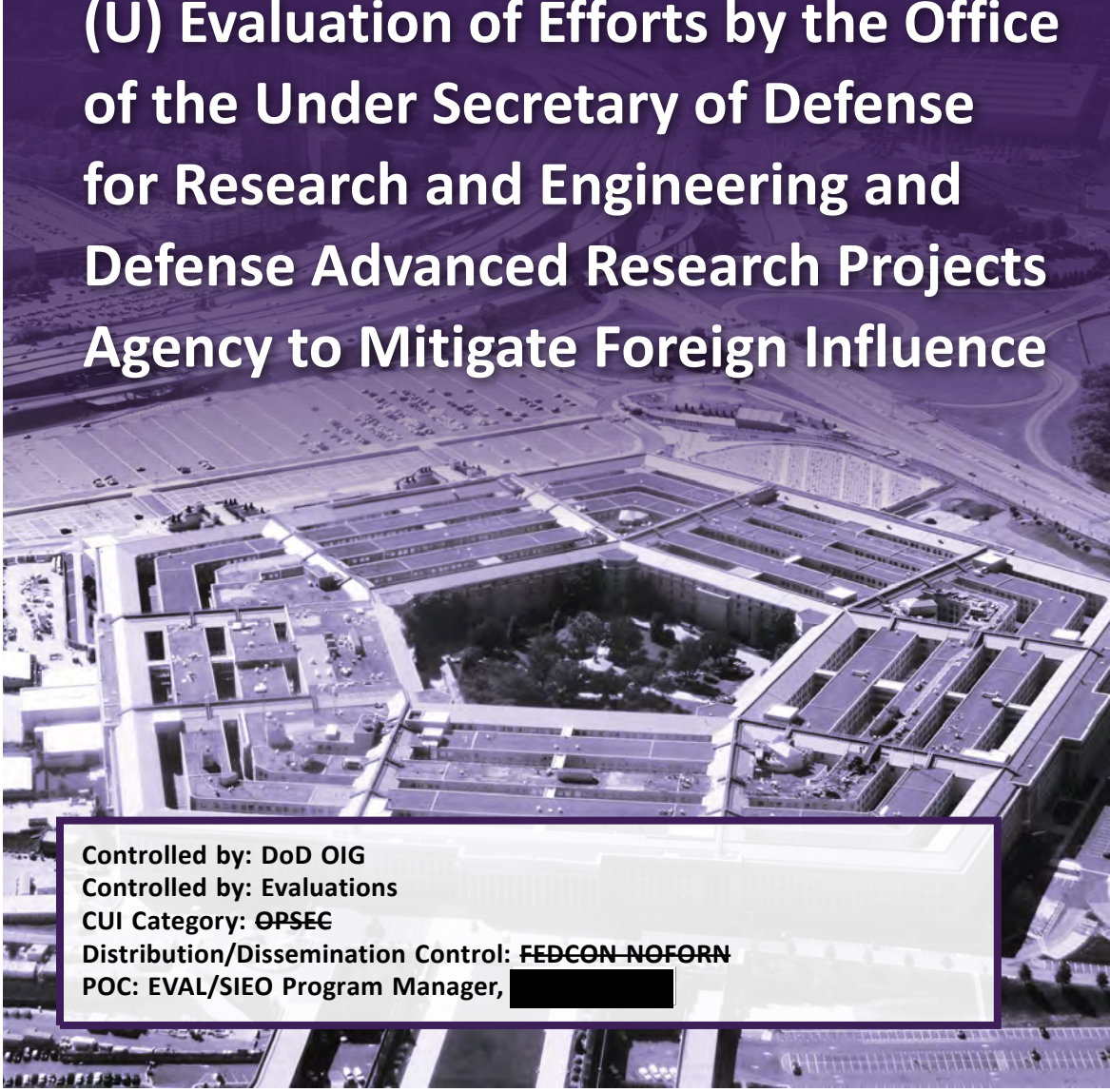
~~CUI//NOFORN~~

INSPECTOR GENERAL

U.S. Department of Defense

JULY 22, 2022

(U) Evaluation of Efforts by the Office of the Under Secretary of Defense for Research and Engineering and Defense Advanced Research Projects Agency to Mitigate Foreign Influence



Controlled by: DoD OIG
Controlled by: Evaluations
CUI Category: ~~OPSEC~~
Distribution/Dissemination Control: ~~FEDCON NOFORN~~
POC: EVAL/SIEO Program Manager, [redacted]

INTEGRITY ★ INDEPENDENCE★ EXCELLENCE

~~CUI//NOFORN~~


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

(U) Results in Brief

(U) Evaluation of Efforts by the Office of the Under Secretary of Defense for Research and Engineering and Defense Advanced Research Projects Agency to Mitigate Foreign Influence

July 22, 2022

(U) Objective

(U) We determined whether the Office of the Under Secretary of Defense for Research and Engineering (OUSD[R&E]) monitored and mitigated foreign influence into the DoD's research and development (R&D) programs. Specifically, we evaluated the implementation and execution of DoD programs by the OUSD(R&E) and Defense Advanced Research Projects Agency (DARPA) to identify and protect critical programs and technologies, and to integrate counterintelligence activities to protect and support R&D in accordance with DoD Directive (DoDD) 5137.02 requirements.[1]

(U) Background

(U) The National Counterintelligence Strategy 2020–2022, written by the National Counterintelligence and Security Center and approved by the President, states that foreign intelligence actors—including nation-states, organizations, and individuals—are employing innovative combinations of traditional spying, economic espionage, and supply chain and cyber operations to gain access to critical infrastructure and steal sensitive information, research, technology, and industrial secrets.[2] The United States Code defines foreign malign influence, in relevant part, as "any hostile effort undertaken by, at the direction of, or on behalf of or with the substantial support of, the

(U) Background (cont'd)

(U) government of a covered foreign country with the objective of influencing, through overt or covert means,... activities of the United States Government."[3]

(U) The National Defense Authorization Act for FY 2017 reestablished the Under Secretary of Defense for Research and Engineering (USD[R&E]) as the chief technology officer of the DoD with the mission of advancing technology and innovation for the DoD. The National Defense Authorization Act gave the USD(R&E) broad responsibility over all DoD R&D, including establishing policy on the DoD's research and engineering, technology development, technology transition, prototyping, experimentation, and developmental testing activities and programs.[4] Also, DoD policy specifies those responsibilities which require the USD(R&E) to establish science and technology and program protection policy to manage technical risk to DoD programs, including R&D, from foreign influence.

(U) Finding

(U) The OUSD(R&E) implemented procedures to monitor and mitigate foreign influence into the DoD's R&D programs by:

- (U) initiating a Science and Technology Protection Working Group,
- (U) developing standardized science and technology protection plan templates, and
- (U) creating modernization priority areas.

~~(CUI//NF)~~ [redacted]

- ~~(CUI//NF)~~ [redacted]

[1] (U) DoDD 5137.02, "Under Secretary of Defense for Research and Engineering (USD[R&E])," July 15 2020.

[2] (U) "National Counterintelligence Strategy of the United States of America," 2020–2022.

[3] (U) Section 3059, title 50, United States Code (50 U.S.C. § 3059). The United States Code defines a "covered foreign country" to include the Russian Federation, the Islamic Republic of Iran, the Democratic People's Republic of Korea, the People's Republic of China, or any other country the Director of the Foreign Malign Influence Response Center determines as appropriate.

[4] (U) Public Law 114–328, "National Defense Authorization Act for FY 2017," December 23, 2016.

(U) Results in Brief

(U) Evaluation of Efforts by the Office of the Under Secretary of Defense for Research and Engineering and Defense Advanced Research Projects Agency to Mitigate Foreign Influence

(U) Finding (cont'd)

- ~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

(U) Recommendations

(U) We recommend that the Director of the DARPA Mission Support Office, in collaboration with the Special Agent in Charge of the NCIS Office of Strategic Support, update the CISP and update the memorandum (U) of agreement reinstating the CISP to comply with DoDI 5200.39 and DoDI O-5240.24 requirements for research, development, and acquisition programs with CPI.

(U) We also recommend that the Director of the DARPA Mission Support Office, in collaboration with the Special Agent in Charge of the NCIS Office of Strategic Support, implement the CISP and memorandum of agreement to comply with DoDI 5200.39 and DoDI O-5240.24 requirements for the DoD research, development, and acquisition programs with CPI.

Management Actions Taken

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

(U) Please see the Recommendations Table on the next page for the status of recommendations.

[5] (U) DoDI 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test and Evaluation (RDT&E)," May 28, 2015 (Incorporating Change 3, October 1, 2020). DoDI O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011 (Incorporating Change 2, July 15, 2020).

[6] ~~(CUI//NF)~~ [redacted]

(U) Recommendations Table

Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Director, Mission Support Office, DARPA	None	None	1.a, 1.b
Special Agent in Charge, Office of Strategic Support, NCIS	None	None	1.a, 1.b

(U) Note: The following categories are used to describe agency management's comments to individual recommendations.

- **(U) Unresolved** – Management has not agreed to implement the recommendation or has not proposed actions that will address the recommendation.
- **(U) Resolved** – Management agreed to implement the recommendation or has proposed actions that will address the underlying finding that generated the recommendation.
- **(U) Closed** – DoD OIG verified that the agreed upon corrective actions were implemented.


INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
INTEGRITY
EFFICIENCY

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

July 22, 2022

(U) MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING
DIRECTOR, DEFENSE ADVANCED RESEARCH PROJECTS AGENCY
DIRECTOR, NAVAL CRIMINAL INVESTIGATIVE SERVICE

(U) SUBJECT: Evaluation of Efforts by the Office of the Under Secretary of Defense for Research and Engineering and the Defense Advanced Research Projects Agency to Mitigate Foreign Influence (Report No. DODIG-2022-113)

(U) This final report provides the results of the DoD Office of Inspector General's evaluation. We considered management's comments on a discussion draft copy of this report when took action to address the recommendations in this report, and we consider the recommendations closed.

(U) We appreciate the cooperation and assistance received during the evaluation. If you have any questions, please contact [redacted]

Randolph R. Stone
Assistant Inspector General
Space, Intelligence, Engineering, and Oversight

(U) Contents

(U) Introduction

(U) Objective

(U) The objective of this evaluation was to determine whether the Office of the Under Secretary of Defense for Research and Engineering (OUSD[R&E]) monitored and mitigated foreign influence into the DoD's research and development (R&D) programs. Specifically, we evaluated the implementation and execution of DoD programs by the OUSD(R&E) and Defense Advanced Research Projects Agency (DARPA) to identify and protect critical programs and technologies, and to integrate counterintelligence (CI) activities to protect and support R&D in accordance with the requirements of DoD Directive (DoDD) 5137.02, "Under Secretary of Defense for Research and Engineering (USD[R&E])."[7]

(U) Background

(U) The National Counterintelligence Strategy of the United States of America 2020–2022, written by the National Counterintelligence and Security Center and approved by the President, states that many countries target the United States because it is a global center for high technology research, technology, and innovation. The National Counterintelligence Strategy also states that foreign intelligence actors—including nation-states, organizations, and individuals—are employing innovative combinations of traditional spying, economic espionage, supply chain, and cyber operations to gain access to critical infrastructure to steal sensitive information, research, technology, and industrial secrets.[8] Although the U.S. Government does not have a comprehensive definition of foreign influence, the United States Code defines foreign malign influence as "any hostile effort undertaken by, at the direction of, or on behalf of or with the substantial support of, the government of a covered foreign country with the objective of influencing, through overt means, … activities of the United States Government."[9]

(U) The National Defense Authorization Act for FY 2017 reestablished the USD(R&E) as the chief technology officer of the DoD with the mission of advancing technology and innovation for the DoD. The National Defense Authorization Act for FY 2017 gave the USD(R&E) broad responsibility over all DoD R&D, including establishing

[7] (U) DoDD 5137.02, "Under Secretary of Defense for Research and Engineering (USD[R&E])," July 15 2020.

[8] (U) "National Counterintelligence Strategy of the United States of America," 2020–2022, January 7, 2020.

[9] (U) Section 3059, title 50, United States Code (50 U.S.C. § 3059). The United States Code defines a "covered foreign country" to include the Russian Federation, the Islamic Republic of Iran, the Democratic People's Republic of Korea [North Korea], the People's Republic of China, or any other country the Director of the Foreign Malign Influence Response Center determines as appropriate. In this report, we use "foreign influence" instead of "Foreign malign influence" because the National Counterintelligence Strategy states that the United States will defend against foreign influence. The Strategy does not define foreign influence specifically. The closest definition to "foreign influence" is "foreign malign influence," defined in 50 U.S.C. § 3059.

(U) policy on the DoD's research and engineering, technology development, technology transition, prototyping, experimentation, and developmental testing activities and programs.[10] DoDD 5137.02 specifies the USD(R&E) responsibilities identified in the National Defense Authorization Act for FY 2017. Specifically, DoDD 5137.02 states that the USD(R&E) is the "principal staff assistant and advisor to the Secretary and Deputy Secretary of Defense for all matters regarding the DoD R&E enterprise," and is responsible for "program and technology protection, as well as program protection planning." Program and technology protection includes establishing science and technology (S&T) and program protection policy to manage technical risk to DoD programs, including R&D.

(U) DoDD 5134.10, "Defense Advanced Research Projects Agency," states that DARPA is a direct reporting agency to the USD(R&E) and serves as the research and development organization in the DoD with primary responsibility for maintaining U.S. technological superiority over U.S. adversaries.[11] Additionally, DARPA is responsible for "identifying, promoting, and sponsoring revolutionary, high-risk, high-payoff R&D to bridge the gap between groundbreaking innovation and military capabilities." To maintain U.S. technological superiority, DARPA relies on DoD S&T and program protection policy and guidance from the USD(R&E).

(U) The following sections discuss the DoD program and technology protection policy and requirements, as well as roles and responsibilities for the DoD Components in program protection for R&D in accordance with DoD policy.

(U) DoD Policy and Program Protection Requirements for Research and Development Activities

(U) The DoD has several policies that require program protection for DoD R&D activities. These policies include DoDD 5137.02; DoD Instruction (DoDI) 5000.83, "Technology and Program Protection to Maintain Technological Advantage"; DoDI 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)"; DoDI O-5240.10, "Counterintelligence in the DoD Components"; and DoDI O-5240.24, "Counterintelligence Activities Supporting Research, Development, and Acquisition."[12]

---

10 (U) Public Law 114–328, "National Defense Authorization Act for FY 2017," December 23, 2016.

11 (U) DoDD 5134.10, "Defense Advanced Research Projects Agency," May 7, 2013 (Incorporating Change 1, September 22, 2017).

12 (U) DoDI 5000.83, "Technology and Program Protection to Maintain Technological Advantage," July 20, 2020 (Incorporating Change 1, May 21, 2021); DoDI 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test and Evaluation (RDT&E)," May 28, 2015 (Incorporating Change 3, October 1, 2020); DoDI O-5240.10, "Counterintelligence (CI) in the DoD Components," April 27, 2020; DoDI O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011 (Incorporating Change 2, July 15, 2020).

(U) DoD Directive 5137.02

(U) DoDD 5137.02 requires the USD(R&E) to coordinate with the Under Secretary of Defense for Intelligence and Security (USD[I&S]) and the Under Secretary of Defense for Acquisition and Sustainment to establish DoD technology protection policy to … "maintain technological advantage and mitigate the exploitation of critical programs and technologies by adversaries." DoDI 5000.83 is the policy by which USD(R&E) establishes DoD technology and program protection as required by DoDD 5137.02.

(U) DoD Instruction 5000.83

(U) DoDI 5000.83 requires S&T managers and engineers to assess technology and program risks to determine program protection measures. For example, technology area protection plans (TAPPs) "are established for each S&T modernization priority area and are designed to reduce compromise or loss of critical technologies and protect against unwanted technology transfer." TAPPs also guide DoD S&T, export controls, international agreements, security, CI, and law enforcement activities.

(U) Additionally, DoDI 5000.83 requires the USD(R&E) to establish and maintain TAPPs and associated policy, guidance, education, and training for designated modernization priorities to achieve horizontal protection.[13] Furthermore, DoDI 5000.83 requires "S&T managers to prepare S&T protection plans as a management tool to guide S&T protection activities."

(U) DoDI 5200.39

(U) DoDI 5200.39 requires DoD Component heads to prepare counterintelligence support plans (CISPs) "for all DoD Component–designated RDT&E facilities and cleared defense contractor facilities with CPI," in accordance with DoDI O-5240.24.[14] A CISP is "a formal and living plan describing activities conducted by a Defense

[13] (U) Horizontal protection is the application of a consistent level of protection to similar critical program information associated with more than one research, development, test, and evaluation program. This includes inherited critical program information, which is owned and generated by one research, development, test, and evaluation program, subsystem, or project and incorporated into and used by another research, development, test and evaluation program.

[14] (U) DoDI O-5240.24 defines cleared defense contractor as "a company or academic institution (i.e. university or college) that has entered into a security agreement with the DoD, and was granted a facility (security) clearance enabling the entity to be eligible for access to classified information of a certain category, as well as all lower categories. DoDI 5200.39 defines CPI as "the U.S. capability elements that contribute to Service members' technical advantage, which, if compromised, undermines U.S. military advantage. U.S. capability elements may include, but are not limited to, software algorithms and specific hardware residing on the applicable system, its training equipment, or maintenance support equipment."

(U) CI Component in support of a DoD [R&D] program or activity with CPI, at DoD-affiliated RDT&E facilities, and at essential cleared defense contractor facilities where CPI resides." A CISP includes, at a minimum, the following elements.

1. (U) Description of the facility, R&D program with CPI, or a cleared defense contractor with CPI: The implementing Defense CI Component, at its discretion, may develop a CISP encompassing all R&D programs with CPI under the cognizance of an RDT&E facility, under the oversight of a program executive office, or for essential cleared defense contractors that support the facility or R&D program where CPI is present.
2. (U) Activities determination: CI activities in a CISP are based on an assessment of the foreign collection threat and the relationship between the threat and vulnerabilities to the CPI. Additionally, CI activities are selected to detect foreign intelligence entity–associated activity.
3. (U) Signature: At a minimum, the CISP is signed by the senior CI person representing the implementing Defense CI Component.

(U) DoDI O-5240.10

~~(CUI//NF)~~ [redacted]

(U) DoDI O-5240.24

~~(CUI//NF)~~ [redacted]

(U) DoD Component Roles and Responsibilities for Program Protection Requirements for R&D Activities

(U) DoD Components have assigned roles and responsibilities as well as specific requirements for program protection of R&D activities in accordance with DoD policies. Specifically, the OUSD(R&E), DARPA, and NCIS have specified roles and responsibilities for protecting R&D programs.

(U) Office of the Under Secretary of Defense for Research and Engineering

(U) As discussed, DoDI 5000.83 requires the USD(R&E) to "establish and maintain S&T and program protection policy, guidance, education, and training to manage technical risk to DoD technical programs." Additionally, DoDI 5000.83 requires the USD(R&E) to "provide advice and make recommendations to the Secretary of Defense on system security engineering matters, including program protection risks to DoD-sponsored research, technology, programs, systems, and capabilities."

(U) Defense Advanced Research Projects Agency

~~(CUI//NF)~~ DoDD 5134.10 assigns the DARPA Director with responsibility for "accelerating the development of [military] capabilities through innovative R&D projects and technology demonstrations." [redacted]

(U) DoDI 5200.39 requires DoD Component heads to "prepare a CISP for all DoD Component–designated RDT&E facilities and defense contractor facilities with CPI" in accordance with DoDI O-5240.24. This means that the DARPA Director, as the DARPA Component head, is required to prepare a CISP for DARPA R&D programs with CPI and document CI activities supporting DARPA's R&D programs with CPI in the CISP.

~~(CUI//NF)~~ [redacted]

(U) Naval Criminal Investigative Service

(U) Secretary of the Navy Instruction (SECNAVINST) 5430.107A identifies NCIS as the Department of the Navy's "civilian federal law enforcement agency that protects and defends the Department of the Navy against terrorism, foreign intelligence threats, and major criminal offenses … and provides law enforcement

(U) and CI services… ."[15] SECNAVINST 5430.107A states that NCIS "will conduct the full range of CI … activities to identify and neutralize the foreign intelligence entity targeting and exploitation… ." In addition, SECNAVINST 5430.107A states that "NCIS will support [R&D] by conducting CI activities that protect CPI, technologies, or systems."

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

[15] (U) Secretary of the Navy Instruction 5430.107A, "Mission and Functions of the NCIS," June 19, 2019.

[16] (U) DoDD 5240.02 defines CI functional services as "CI activities conducted to support the four missions of CI and that enable one or more of the other CI functions." The four CI missions are: countering espionage, international terrorism, and the CI insider threat; support to force protection; support to defense critical infrastructure program; and support to research, development, and acquisition.

~~(CUI//NF)~~ [redacted]

[17] (U) DoDI O-5240.24 requires the MDCO to prepare a CISP for R&D programs with CPI. DoDI O-5240.10 requires the MDCO to prepare a MOA with the supported component headquarters documenting CI support provided to the component.

(U) Finding

~~(CUI//NF)~~ [redacted]

(U) The OUSD(R&E) implemented procedures that support DoDD 5137.02 requirements for program and technology protection to monitor and mitigate foreign influence into the DoD's R&D programs by:

- (U) initiating an S&T Protection Working Group,
- (U) developing standardized S&T protection plan templates, and
- (U) creating modernization priority areas.

(U) However,

- ~~(CUI//NF)~~ [redacted]
- ~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

(U) The OUSD(R&E) Implemented Procedures to Monitor and Mitigate Foreign Influence

(U) The OUSD(R&E) implemented procedures that support DoDD 5137.02 requirements for program and technology protection to monitor and mitigate foreign influence by:

- (U) initiating the S&T Protection Working Group,
- (U) developing standardized S&T protection plan templates, and
- (U) creating modernization priority areas.

(U) The OUSD(R&E) Initiated the Science and Technology Protection Working Group

(U) On August 12, 2021, the OUSD(R&E) S&T Protection Director told us that the OUSD(R&E) formed the S&T Protection Working Group in November 2019 to gather community feedback on established DoD guidance for monitoring and mitigating foreign influence. Although DoD policy does not require the OUSD(R&E) to establish an S&T Protection Working Group, the activity does bring together the DoD R&D and Defense Intelligence communities. The S&T Protection Director told us that although the S&T Protection Working Group operates without a charter, the group has monthly meetings and participation in the meetings is robust throughout the DoD.

(U) We reviewed S&T Protection Working Group meeting notes from January 2021 to May 2021 to verify that participation in the meetings was representative of many organizations throughout the DoD. We identified that personnel from multiple Office of the Secretary of Defense Components, the Defense Intelligence Enterprise, the Military Services' research labs, and intelligence and Defense CI Components participated in S&T Protection Working Group meetings. In addition, on May 20, 2021, a DoD OIG team member participated in the S&T Protection Working Group teleconference and observed participants discussing guidance for monitoring and mitigating foreign influence. For example, attendees discussed technology decomposition, which is the essential technology elements needed for criticality analysis.[18] The S&T Protection Working Group attendees also discussed draft updates to DoDI 3210.7, "Research Integrity and Misconduct," including implementation of the requirements in National Security Presidential Memorandum-33 for conflicts of interest and conflicts of commitment for

[18] (U) Essential technology elements are knowledge, processes, material, hardware, or software developed from engineering or applied sciences that have the potential to contribute to a U.S. military or economic lethal advantage over a strategic competitor. Essential technology elements consist of scientific technology information, controlled technical information, or a combination of enabling technologies that are necessary to achieve a critical DoD military capability.

(U) performers on grants or contracts.[19] The attendees also identified shortfalls in the draft updates to DoDI 3210.7. For example, the updates did not identify the DoD Components or organizations that would be responsible for mitigating foreign influence.

(U) The OUSD(R&E) Developed a Standardized Science and Technology Protection Plan Template

(U) The OUSD(R&E) developed a standardized S&T protection plan template to inform S&T managers on best practices that may be adopted based on their organizational needs and R&D program requirements. Although the S&T protection plan template is not required by DoD policy, standardized S&T protection plans help the DoD R&D community. The distribution of the S&T protection plan template to the DoD R&D community provides an additional measure to protect DoD R&D programs from foreign influence by standardizing how S&T protection plans are created. R&D program-specific requirements dictate what will be included in an organization's S&T protection plan. The S&T protection plan facilitates discussions among S&T managers, technology subject matter experts, security staff, CI representatives, and intelligence analysts on a range of threat scenarios. The S&T protection plan also formulates appropriate countermeasures to protect R&D programs.

(U) DoDI 5000.83 states that the S&T protection plan must document, at a minimum:

1. (U) essential technology elements and enabling technologies;
2. (U) threats to, and vulnerabilities of, the essential technology elements; and
3. (U) selected countermeasures to mitigate associated risks.

(U) We reviewed the S&T protection plan template and determined that the template includes the minimum requirements of DoDI 5000.83. For example, the template recommends that S&T protection plans include sections for introduction; updates; responsible points of contact; technology element identification and risk assessment; identified threats and vulnerabilities; countermeasures and risk mitigation plan; and response, recovery, and support.

[19] (U) DoDI 3210.7, "Research Integrity and Misconduct," May 14, 2004 (Incorporating Change 1, October 15, 2018). The Instruction specifies the procedures and standards for the DoD for the prevention of research misconduct. National Security Presidential Memorandum-33, "Presidential Memorandum on United States Government-Supported Research and Development National Security Policy," January 14, 2021.

(U) The OUSD(R&E) Created Modernization Priority Areas to Focus Protection Actions

(U) The OUSD(R&E) created a list of modernization priority areas to unify and advance the Department's investments and capabilities in that area. As a result, the Department is also able to focus protection efforts for technologies critical to military capabilities. Although the modernization priority areas are not required by DoD policy, DoDI 5000.83 requires the USD(R&E) to create and maintain technology area protection plans (TAPP) for each of the modernization priority areas. We reviewed the modernization priority areas and identified that they include space, cyber, hypersonics, 5G, microelectronics, autonomy, biotechnology, directed energy, quantum science, networked communications, and artificial intelligence. The S&T Protection Director stated that the modernization priority areas evolved from a critical program technology list that was based on military requirements for the National Defense Strategy.

(U) In addition to focusing protection resources, DoDI 5000.83 requires a TAPP for each modernization priority area to reduce the risk of compromise or loss of critical technologies. The TAPP protects against unwanted technology transfer. We reviewed and verified that the OUSD(R&E) developed TAPPs for each of the DoD modernization priority areas. Therefore, the OUSD(R&E) complied with the DoDI 5000.83 requirement.

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted].

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted].

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

- [redacted]
- [redacted]

(CUI//NF) [redacted]

~~(CUI//NF)~~ [redacted]

- ~~(CUI//NF)~~ [redacted]

[20] ~~(CUI//NF)~~ [redacted]

- ~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~***(CUI//NF)***~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]:

- ~~(CUI//NF)~~ [redacted]
- ~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

- ~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

- ~~(CUI//NF)~~ [redacted]
- ~~(CUI//NF)~~ [redacted]

~~(CUI//NF)~~ [redacted]

(U) Recommendation

(U) Recommendation 1

(U) We recommend that the Director of the Mission Support Office, Defense Advanced Research Projects Agency, in collaboration with the Special Agent in Charge of the Office of Strategic Support, Naval Criminal Investigative Service:

a. ~~**(CUI//NF)**~~ [redacted]

b. ~~**(CUI//NF)**~~ [redacted]

~~(CUI//NF)~~ [redacted]

(U) Management Actions Taken

~~(CUI//NF)~~ [redacted]

(U) Appendix

(U) Scope and Methodology

(U) We conducted this evaluation from May 2021 through May 2022 in accordance with the "Quality Standards for Inspection and Evaluation," published in January 2012 by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we adequately plan the evaluation to ensure that objectives are met and that we perform the evaluation to obtain sufficient, competent, and relevant evidence to support the findings, conclusions, and recommendations. We believe that the evidence obtained was sufficient, competent, and relevant to lead a reasonable person to sustain the findings, conclusions, and recommendations.

(U) This report was reviewed by the DoD Components associated with this oversight project to identify whether any of their reported information, including legacy FOUO information, should be safeguarded and marked in accordance with the DoD CUI Program. In preparing and marking this report, we considered any comments submitted by the DoD Components about the CUI treatment of their information. If the DoD Components failed to provide any or sufficient comments about the CUI treatment of their information, we marked the report based on our assessment of the available information.

~~(CUI//NF)~~ [redacted]

(U) To complete our evaluation, we conducted teleconferences, interviews, and requests for information from senior leadership, policy advisors, and CI special agents at the following organizations who are responsible for protecting DoD R&D from foreign influence.

- (U) OUSD(R&E)
- (U) OUSD(I&S)
- (U) DARPA
- (U) Defense Counterintelligence and Security Agency
- (U) NCIS

(U) We collected testimonial and documentary evidence from each of the DoD organizations listed above, including:

- (U) criteria, policies, procedures for roles and responsibilities for protecting DoD R&D;
- (U) criteria, policies, and procedures of requirements for protecting DoD R&D;
- (U) examples of procedures on how foreign influence is mitigated;
- (U) contracts, contract modifications, budget, and Small Business Innovation Research documents concerning the material for the extreme environments project; and
- (U) S&T Protection Working Group meeting notes.

(U) We reviewed contracts, contract modifications, and Small Business Innovation Research documents to determine whether mitigation measures were being included in high-priority contracts to mitigate foreign influence in DoD R&D. Additionally, we reviewed CI support to R&D documents and compared the CISP to the MOA and the requirements of each.

(U) We also reviewed laws and DoD policies to determine whether the DoD Components were following the policies for protecting DoD R&D. These include the following documents:

- (U) DoDI 5000.83, "Technology and Program Protection to Maintain Technological Advantage," July 20, 2020 (Incorporating Change 1, May 21, 2021)
- (U) DoDI 5200.39, "Critical Program Information (CPI) Identification and Protection within Research, Development, Test, and Evaluation (RDT&E)," May 28, 2015 (Incorporating Change 3, Effective October 1, 2020)
- (U) DoDI O-5240.10, "Counterintelligence in the DoD Components," April 27, 2020
- (U) DoDI O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011 (Incorporating Change 2, Effective July 15, 2020)
- (U) DoDI 4000.19, "Support Agreements," December 16, 2020

(U) Use of Computer-Processed Data

(U) We did not use computer-processed data to perform this evaluation.

(U) Prior Coverage

(U) During the last 5 years, the Government Accountability Office (GAO) issued two reports discussing foreign influence. Unrestricted GAO reports can be accessed at http://www.gao.gov.

(U) GAO

(U) Report No. GAO-21-158, "DoD Critical Technology: Plans for Communicating, Assessing, and Overseeing Protection Efforts Should Be Completed," January 2021

> (U) The GAO report stated that the DoD had outlined a revised process to better identify and protect its critical technologies including those associated with acquisition programs throughout their lifecycle or those early in development. The GAO recommended that the DoD specify how it will communicate its critical programs and technology list, develop metrics to assess protection measures, and select the DoD organization that will oversee protection efforts beyond 2020.

(U) Report No. GAO-21-130, "Federal Research: Agencies Need to Enhance Policy to Address Foreign Influence," December 2020

(U) The GAO report stated that U.S. research may be subject to undue foreign influence in cases where a researcher has a foreign conflict of interest. The GAO recommended that the Secretary of Defense develop an agency-wide policy on conflict of interest for grants, to address both financial and non-financial conflicts, and that the Secretary of Defense document procedures, including roles and responsibilities for addressing and enforcing failures to disclose required information, both foreign and domestic.

(U) DoD OIG

(U) Report No. DODIG-2022-086, "Evaluation of the Defense Logistics Agency Lifetime Buys of Parts Used in Intelligence, Surveillance, and Reconnaissance Systems," April 19, 2022

> (U) This report contains controlled unclassified information.

(U) Report No. DODIG-2020-106, "Evaluation of Security Controls for Intelligence, Surveillance, and Reconnaissance System Supply Chains," July 22, 2020

> (U) This report provided recommendations regarding the DoD's Supply Chain Resource Management Threat Analysis Center and the Defense Counterintelligence and Security Agency. The report is classified.

(U) Acronyms and Abbreviations

CI	Counterintelligence (lowercase in text)
CISP	Counterintelligence Support Plan (lowercase in text)
CPI	Critical Program Information (lowercase in text)
DARPA	Defense Advanced Research Program Agency
DoDD	DoD Directive
DoDI	DoD Instruction
MDCO	Military Department Counterintelligence Organization
MOA	Memorandum of Agreement (lowercase in text)
NCIS	Naval Criminal Investigations Service
OUSD(R&E)	Office of the Under Secretary of Defense for Research and Engineering
R&D	Research and Development (lowercase in text)
RDT&E	Research, Development, Test, and Evaluation (lowercase in text)
S&T	Science and Technology (lowercase in text)
TAPP	Technology Area Program Protection (lowercase in text)
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(R&E)	Under Secretary of Defense for Research and Engineering


INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
INTEGRITY
EFFICIENCY

Whistleblower Protection
U.S. Department of Defense

Whistleblower Protection safeguards DoD employees against retaliation for protected disclosures that expose possible fraud, waste, and abuse in Government programs. For more information, please visit the Whistleblower webpage at http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whisteblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

For more information about DoD OIG reports or activities, please contact us:

Congressional Liaison
703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

DoD OIG Mailing Lists
www.dodig.mil/Mailing-Lists/

Twitter
www.twitter.com/DoD_IG

DoD Hotline
www.dodig.mil/hotline

DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, Virginia 22350-1500
www.dodig.mil
DoD Hotline 1.800.424.9098