

CUI//SP-CTI



# INSPECTOR GENERAL

*U.S. Department of Defense*

OCTOBER 4, 2024



## (U) Audit of Space Force's Implementation of Software Assurance for the Next Generation Overhead Persistent Infrared Program

**Controlled by:** DoD-OIG  
**Controlled by:** Audit/Cyberspace Operations  
**CUI Category:** Controlled Technical Information, DoD Critical Infrastructure Security Information  
**Distribution/Dissemination Control:** FEDCON  
**Distribution Statement:** C  
**POC:** Assistant Inspector General for Audit, Cyberspace Operations,  
[REDACTED]

**Distribution Statement C.** Distribution authorized to U.S. Government agencies and their contractors; CTI; 01 JUL 2024. Other requests for this document must be referred to DoD Office of Inspector General, Assistant Inspector General for Audit, Cyberspace Operations, 4800 Mark Center Drive, Alexandria, VA 22350.

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY

CUI//SP-CTI





# (U) Results in Brief

## (U) Audit of Space Force's Implementation of Software Assurance for the Next Generation Overhead Persistent Infrared Program

October 4, 2024

### (U) Objective

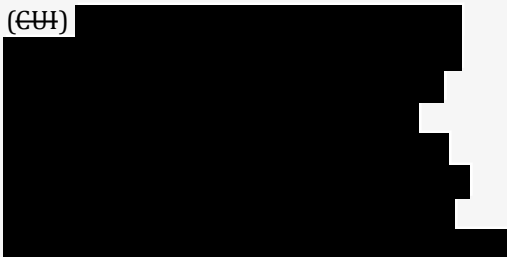
(U) The objective of this audit was to determine whether the Next Generation Overhead Persistent Infrared (Next Gen OPIR) program management office (PMO) was effectively implementing software assurance (SwA) to identify and mitigate vulnerabilities in system software.

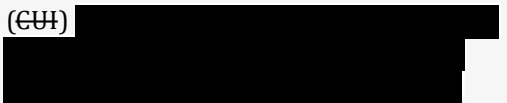
### (U) Background

(U) SwA is the level of confidence that software functions only as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software.

(U) The Next Gen OPIR Program is a space-based, strategically survivable missile warning satellite system designed to counter current and future threats in a contested space environment. We reviewed the SwA activities conducted for three software-dependent components within the Next Gen OPIR Geosynchronous Earth Orbit (GEO) space vehicles' (satellites') mission payload module.

### (U) Findings

(U)   
In addition, PMO officials did not ensure that the program protection plan (PPP) was consistently updated.

(U) 

### (U) Findings (cont'd)

(U) 

(U) DoD guidance allows program managers to tailor program protection planning procedures, including SwA, based on the characteristics of the required capability and the associated risk. However, the risk accepted by not conducting or completing an SwA activity is not required to be detailed in the PPP, which results in an incomplete risk profile.

(U) If PMO officials do not ensure that SwA is sufficiently completed during software development, there is an increased risk that the software may include vulnerabilities that could prevent the GEO satellites from performing their mission. If the PPP does not reflect the risk acceptance associated with SwA and is not reviewed and updated annually, then the Milestone Decision Authority will not be fully informed of program risk.

### (U) Recommendations

(U) We recommend that the Under Secretary of Defense for Research and Engineering revise PPP guidance to include a process for the identification of software assurance risks and steps for how the acceptance of risks should be tracked, if left unmitigated.

(U) 

### (U) Management Comments and Our Response

(U) The Under Secretary of Defense for Research and Engineering and the Next Gen OPIR Program Manager did not provide comments on the recommendations. Therefore, the recommendations are unresolved and we request comments on the recommendations within 30 days. Please see the Recommendations Table on the next page.

### **(U) Recommendations Table**

(U) Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
(U) Under Secretary of Defense for Research and Engineering	1	None	None
(U) Next Generation Overhead Persistent Infrared Program Manager	2.a, 2.b, 2.c, 2.d, 3.a, 3.b	None	None  (U)

(U) Please provide Management Comments by November 4, 2024.

**(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** – The DoD OIG verified that the agreed upon corrective actions were implemented.



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

October 4, 2024

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR RESEARCH  
AND ENGINEERING  
ASSISTANT SECRETARY OF THE AIR FORCE FOR SPACE  
ACQUISITION AND INTEGRATION  
COMMANDER, SPACE SYSTEMS COMMAND  
AUDITOR GENERAL, DEPARTMENT OF THE AIR FORCE

SUBJECT: (U) Audit of the Space Force's Implementation of Software Assurance for the Next Generation Overhead Persistent Infrared Program (Report No. DODIG-2025-001)

(U) This final report provides the results of the DoD Office of Inspector General's audit. We previously provided copies of the draft report and requested written comments on the recommendations. We were not able to consider management's comments on the draft report when preparing the final report because comments were not provided.

(U) This report contains seven recommendations that are considered unresolved because the Under Secretary of Defense for Research and Engineering and the Next Generation Overhead Persistent Infrared Program Manager did not provide comments on the recommendations. We will track these recommendations until management has agreed to take actions that we determine to be sufficient to meet the intent of the recommendations and management officials submit adequate documentation showing that all agreed-upon actions are completed.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. Therefore, within 30 days, please provide us your response concerning specific actions in process or alternative corrective actions proposed on the unresolved recommendations. Send your response to either [followup@dodig.mil](mailto:followup@dodig.mil) if unclassified or [rfunet@dodig.smil.mil](mailto:rfunet@dodig.smil.mil) if classified SECRET.

(U) If you have any questions, please contact me at [REDACTED]. We appreciate the cooperation and assistance received during this audit.

FOR THE INSPECTOR GENERAL:

A handwritten signature in cursive script that reads "Carol N. Gorman".

Carol N. Gorman  
Assistant Inspector General for Audit  
Cyberspace Operations

# (U) Contents

---

## (U) Introduction

(U) Objective ..... 1

(U) Background ..... 1

**(CUI)** [REDACTED] ..... 7

(U) PMO Officials Ensured that Design Inspection, Code Inspection, CVE, CWE, and Test Coverage Were Completed, and Penetration Testing Planned ..... 8

**(CUI)** [REDACTED] ..... 9

**(CUI)** [REDACTED] ..... 11

(U) PMO Officials Are Authorized to Tailor SwA Activities Based on Risk But the PPP Does Not Have to Reflect the Risk Acceptance ..... 12

**(CUI)** [REDACTED] ..... 13

(U) Recommendations, Management Comments, and Our Response ..... 14

## (U) Appendix

(U) Scope and Methodology ..... 16

(U) Internal Control Assessment and Compliance ..... 17

(U) Use of Computer-Processed Data ..... 17

(U) Use of Technical Assistance ..... 18

(U) Prior Coverage ..... 18

**(U) Acronyms and Abbreviations** ..... 21

# (U) Introduction

## (U) Objective

(U) The announced objective of this audit was to determine whether DoD program management offices (PMOs) were implementing software assurance (SwA) countermeasures to mitigate software vulnerabilities throughout the weapon systems acquisition life cycle. During the audit, we revised the objective to focus on the implementation of SwA for the Space Force’s Next Generation Overhead Persistent Infrared (Next Gen OPIR) program.<sup>1</sup> The revised objective of this audit was to determine whether the Space Force’s Next Gen OPIR PMO was effectively implementing SwA to identify and mitigate vulnerabilities in system software.<sup>2</sup> See the Appendix for the scope, methodology, and prior audit coverage.

## (U) Background

(~~EUH~~) DoD weapon systems rely on software, and the secure and rapid development of that software, to maintain a competitive advantage. The DoD’s reliance on software presents opportunities for adversaries to gain unauthorized access to, and corrupt, weapon systems components by exploiting software vulnerabilities. Exploitation of DoD weapon systems through their software can lead to severe consequences for U.S. warfighting capabilities because many defense systems are interconnected. SwA is the level of confidence that software functions as intended and is free of vulnerabilities, either intentionally or unintentionally designed or inserted as part of the software. SwA activities include actions taken to identify vulnerabilities in system software and the countermeasures taken to negate or mitigate an adversary’s ability to exploit those vulnerabilities.■

(U) In accordance with DoD Instruction (DoDI) 5200.44, DoD’s policy is to protect mission critical functions through trusted systems and networks processes, tools, and techniques, including software assurance, throughout the entire system life cycle. Accordingly, PMOs are required to implement SwA throughout a weapon system’s acquisition life cycle to counter adversarial threats that may target

<sup>1</sup> (U) The Next Gen OPIR program was initiated in June 2018 as an Air Force program. After the Space Force was established on December 20, 2019, as a new branch of the Armed Forces within the Department of the Air Force, the Next Gen OPIR program was transitioned to the Space Force.

<sup>2</sup> (U) This report contains information that has been redacted because it was identified by the Department of Defense as Controlled Unclassified Information (CUI) that is not releasable to the public. CUI is Government-created or owned unclassified information that allows for, or requires, safeguarding and dissemination controls in accordance with laws, regulations, or Government-wide policies.

■ (~~EUH~~) [Redacted]

(U) software.<sup>4</sup> The Instruction also requires DoD PMOs to design and conduct SwA activities in the software development, integration, and test phases of systems engineering to mitigate attacks against the system and address potential and actual threats. DoD Instructions 5000.83 and 5000.90 were issued in July and December 2020, respectively, as guidance for technology protection and cybersecurity, including SwA.<sup>5</sup> DoDI 5000.83 and 5000.90 require PMOs to assess and plan for SwA vulnerabilities and remediation strategies. DoDI 5000.83 also requires PMOs to use automated SwA tools to detect vulnerabilities and include remediation actions in the Program Protection Plan (PPP).

### ***(U) Program Protection Plan***

(U) The PPP is a security-focused document that PMOs use throughout the acquisition life cycle to manage security risks to critical program information and mission-critical functions and components. Critical program information includes software algorithms, certain hardware, training or maintenance support equipment, and mission-critical components such as hardware, software, and firmware that implement essential system functions. DoDI 5000.83 requires PMOs to update the PPP throughout the weapon system life cycle and submit the PPP for the approval of the Milestone Decision Authority (MDA), or an equivalent authorizing official at major acquisition pathway decision points.<sup>6</sup> The MDA has overall responsibility for a program, has the authority to approve entry of an acquisition program into the next phase of the acquisition process, and is accountable for cost, schedule, and performance reporting to higher authorities, including Congress. As part of the milestone approval process, the MDA reviews program documentation, including the PPP, to determine whether a program will meet established cost, schedule, and performance milestones.

(U) PPP Outline and Guidance provides DoD PMOs with instructions for developing PPPs.<sup>7</sup> The Guidance requires PMOs to address responsibilities for planning and implementing program protection measures, including SwA, in PPPs. The Guidance includes a SwA Countermeasures Table, with which the PMOs are required to develop goals for conducting SwA and track progress toward meeting those goals

<sup>4</sup> (U) DoDI 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012, Incorporating Change 3, Effective October 15, 2018. The DoDI was revised on February 16, 2024. However, the provisions referred to in the cited version of the DoDI were not significantly changed.

<sup>5</sup> (U) DoDI 5000.83, "Technology and Program Protection to Maintain Technological Advantage," July 20, 2020; and DoDI 5000.90, "Cybersecurity for Acquisition Decision Authorities and Program Managers," December 31, 2020.

<sup>6</sup> (U) Acquisition pathway decision points include milestones that mark transitions between each phase of the DoD acquisition life cycle, and following the completion of technical reviews, in which PMOs demonstrate the technical maturity of the program. Traditional DoD acquisition milestones are: Milestone A, which approves entry into the technology maturation and risk reduction phase; Milestone B, which approves entry into the engineering and manufacturing development phase; and Milestone C, which approves entry into the production and deployment phase.

<sup>7</sup> (U) Deputy Assistant Secretary of Defense for Systems Engineering, "PPP Outline and Guidance," Version 1.0, July 2011.



(U) by updating the Table with actual results at major acquisition milestones. The SwA Countermeasures Table is separated into three sections—Development Process, Operational System, and Development Environment.

**(U) Development Process.** This section is used to identify, set goals for, and track SwA countermeasures conducted during the software development process to mitigate and minimize attacks that the developed system is likely to face when deployed.

**(U) Operational System.** This section is used to record the countermeasures and other SwA activities applied within the operational environment to mitigate attacks against the delivered system and software interfaces in an operational environment.

**(U) Development Environment.** This section is used to record the SwA activities and controls applied to tools and activities used to develop and sustain software to mitigate attacks. Software tools used in the development environment are another source of risk to warfighting capability. For example, an attacker could insert malicious code, exploitable vulnerabilities, and software backdoors into the operational software before it is fielded through the development environment.

(U) Although the SwA Countermeasures Table includes specific SwA activities for each of the sections, DoDI 5000.83 and the SwA Countermeasures in Program Protection Planning guidance allow the Program Manager to tailor program protection planning procedures, including SwA, based on the characteristics and risk profile of the capability being acquired, and the anticipated risks the program will encounter.

### ***(U) Next Generation Overhead Persistent Infrared Program***

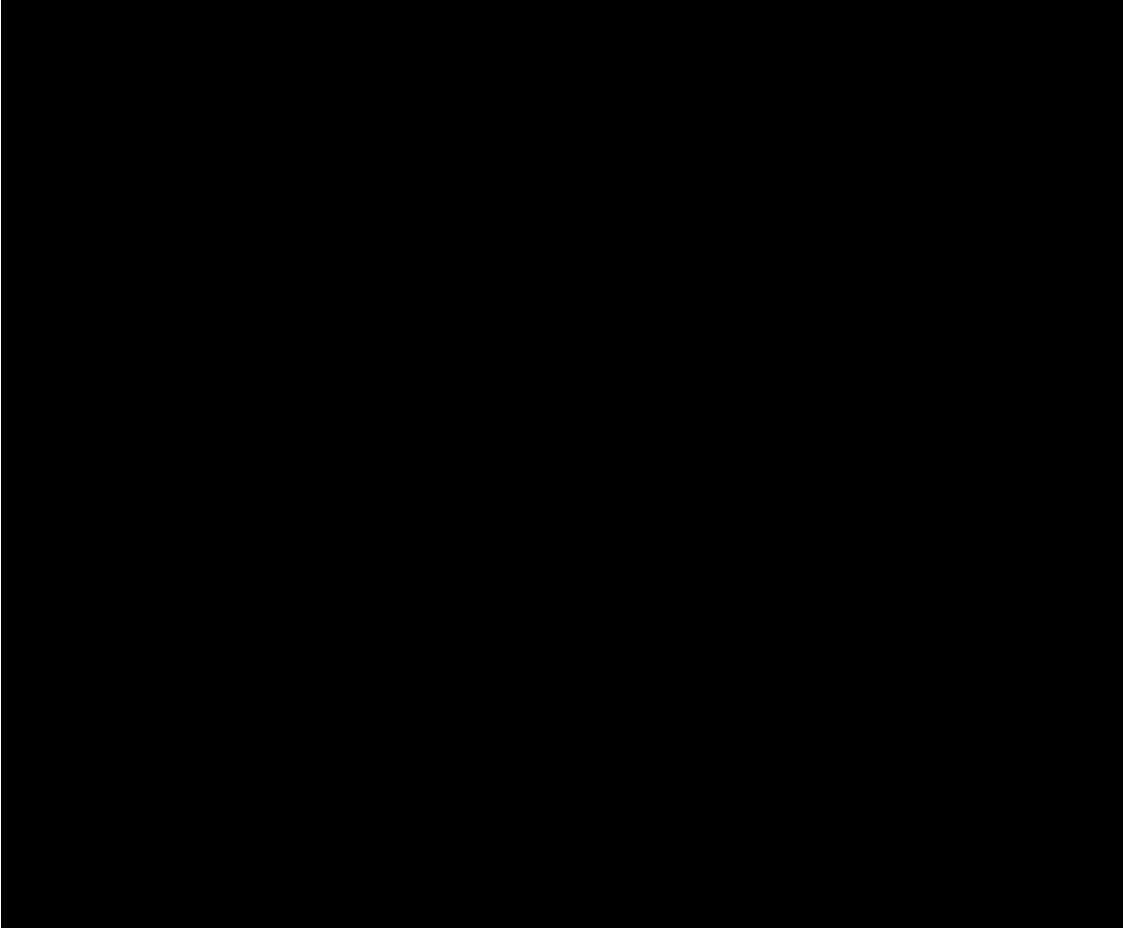
(U) In March 2018, the Department of the Air Force initiated the Next Gen OPIR Program to develop a space-based, strategically survivable missile warning satellite system to counter current and future threats in a contested space environment. The Next Gen OPIR system, once fully operational as designed, will consist of four satellites and one ground station. Specifically, the system will include:

- (U) two Geosynchronous Earth Orbit (GEO) space vehicles (satellites) covering Earth's mid-latitudes,<sup>8</sup>
- (U) two Polar space vehicles in high elliptical orbit covering Earth's upper regions, and

<sup>8</sup> (U) The Next Gen OPIR system initially included plans to develop and deploy three GEO satellites. However, funding for the third GEO satellite was removed from the contract.

- (U) one Future Operationally Resilient Ground Evolution ground station intended to provide DoD decision-makers and Service members with enhanced ground processing and communications capabilities regarding missile threats.

(U) [REDACTED]



(U) [REDACTED]

(U) The Assistant Secretary of the Air Force for Space Acquisition and Integration is the MDA for the Next Gen OPIR and the Senior Materiel Leader, Strategic Missile Warning Acquisition Delta, is the Program Manager. The Department of the Air Force (DAF) System Security Engineering Cyber Guidebook (SSECG) states that the Program Manager is responsible for SwA and for reviewing and coordinating the PPP with the appropriate stakeholders. The SSECG also states that the systems security engineer is responsible for ensuring that SwA is implemented, and that the PPP remains current and updated. Furthermore, the SSECG requires that the PPP for DAF mission critical information systems (space and weapon systems), be reviewed and updated annually.

## **(U) Next Gen OPIR Program Components Reviewed**

(U) We selected for review three software-dependent components that operate in the Next Gen OPIR GEO satellites' mission payload module. We focused on the SwA activities conducted during the Development Process for that software because, at the time of our review, the Next Gen OPIR PMO and contractor software developers had completed most of the program's software development. The PPP Outline and Guidance and Software Assurance Countermeasures in Program Protection Planning define the following SwA activities that should be conducted in the Development.<sup>9</sup>

**(U) Static Analysis** – analyze source code using automated tools to detect coding errors, insecure coding constructs, and other indicators of vulnerabilities or weaknesses that are detectable at the source code level.

**(U) Design Inspection** – review software to identify bugs or defects during the initial stages of the software development life cycle.

**(U) Code Inspection** – test software code to identify errors.

**(U) Common Vulnerabilities and Exposures (CVE)** – compare vulnerabilities to a list of known information security issues using automated scanning tools.

**(U) Common Attack Pattern Enumeration and Classification (CAPEC)** – scan software against a list of attack methods used to exploit weaknesses and vulnerabilities.<sup>10</sup>

**(U) Common Weakness Enumeration (CWE)** – categorize weaknesses identified for hardware and software to facilitate the effective use of automated tools that can identify, fix, and prevent those weaknesses and vulnerabilities.

**(U) Penetration Testing** – attempt to circumvent or defeat the security features of an information system.

**(U) Test Coverage** – provide standards in units or metrics for test completeness (such as percentage of statements exercised, and number of function points tested).

<sup>9</sup> (U) Deputy Assistant Secretary of Defense for Systems Engineering and DoD Chief Information Officer, "Software Assurance Countermeasures in Program Protection Planning," March 2014.

<sup>10</sup> (U) An attack pattern is the common approach and attributes related to the exploitation of a weakness in a software, firmware, hardware, or service component.

(U) In August 2018, the Next Gen OPIR program issued a two-phased, Sole Source Cost Plus Incentive Fee contract, for the development and support of the GEO satellites. As of May 2024, acquisition costs associated with the GEO satellite contract were over \$7 billion. The contract includes requirements for the contractor to integrate SwA into the test and evaluation activities and develop a test and evaluation plan that details its approach for implementing SwA. On October 11, 2023, the GEO satellite contractor issued the GEO Cyber Test and Evaluation (CT&E) Plan, which includes the approach for implementing SwA.

## (U) Finding

(CUI)

(CUI) PMO officials ensured that the GEO satellite contractor completed the design inspection, code inspection, CVE, CWE, and test coverage SwA activities for the software we reviewed in accordance with the CT&E Plan and that plans were in place for the contractor to conduct penetration testing consistent with the software testing schedule. [REDACTED]

- (CUI) [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]<sup>11</sup>
- (CUI) [REDACTED]  
[REDACTED]  
[REDACTED]

(U) DoD Instruction 5000.83 and SwA Countermeasures in Program Protection Planning allow the Program Manager to tailor program protection planning procedures, including SwA, based on the characteristics of the capability being required and the associated risk. However, the risk accepted by not conducting or completing an SwA activity is not required to be detailed in the PPP, which results in an incomplete risk profile. Furthermore, for the GEO satellite software we reviewed, PMO officials did not ensure that the PPP was consistently updated to reflect the contractor’s progress implementing SwA and had not submitted the PPP for MDA approval since October 2020.

(U) If PMO officials do not ensure that SwA is sufficiently completed during software development, there is an increased risk that the software may include vulnerabilities that could prevent the GEO satellites from performing their mission. Furthermore, if the PPP does not reflect the risk acceptance associated with SwA and is not reviewed and updated annually, the MDA will not be fully informed

<sup>11</sup> (U) AFRL is the primary scientific research and development center for the DAF. The AFRL Integration Test & Evaluation Center performed an independent, information system security control assessment of the GEO satellite software to validate cybersecurity maturity during the software development process.

(U) of the program risk and cannot rely on the PPP as part of their assessment to determine whether programs will meet cost, schedule, and performance milestones or that they are ready to transition to the next phase of the acquisition lifecycle.

### **(U) PMO Officials Ensured that Design Inspection, Code Inspection, CVE, CWE, and Test Coverage Were Completed, and Penetration Testing Planned**

(U) PMO officials for the Next Gen OPIR program ensured that the contractor completed the design inspection, code inspection, CVE, CWE, and test coverage SwA activities for the software we reviewed, in accordance with the GEO CT&E Plan and that plans were in place for the contractor to conduct penetration testing consistent with the software testing schedule. For each of the SwA activities, we reviewed the supporting documentation that the contractor provided to the PMO officials to ensure that it was complete and verified that the contractor conducted the SwA activity in accordance with that documentation.

(U) For example, we verified that the contractor conducted and completed code inspection by obtaining and reviewing the results of the contractor's code collaborator tool provided to the PMO.<sup>12</sup> We analyzed the code collaborator tool to verify that the contractor conducted manual software code reviews and notified the software code developers when defects in the source code were identified. We also verified that the contractor monitored the developer's progress toward resolving the defects through a review of the comments and interactions between the developers and reviewers that indicated the reviewers approved the changes made by the developers to address the code defects. We verified that all defects identified by the reviewers were corrected by the developers, which is required for a review to be complete. Specifically, we reviewed the contractor's code and unit checklists, which were completed during the quality assurance process, to verify there were no discrepancies remaining between the code reviewers and developers. Lastly, we confirmed that the contractor attached documentation to the checklists that supported the changes made to the source code.

~~(U)~~ For design inspection, we verified that the contractor conducted and completed the SwA activity by reviewing the software design documentation provided to and approved by the PMO.<sup>13</sup> We verified that the contractor established performance, architectural and interface design, development, and test requirements for the

<sup>12</sup> (U) The contractor used an industry tool used for the peer review of code. The tool is designed to allow developers to share code; annotate, comment, and discuss changes; help to identify and correct bugs; improve the quality of code; and ensure consistency.

<sup>13</sup> (U) Designs and documentation include software design description, interface design, software requirements specifications, and software product assessments.

(CUI) software we reviewed. [REDACTED]

We reviewed presentations from the contractor to PMO officials and confirmed that PMO officials approved final designs, further ensuring software functionality and appropriate protections. Additionally, we reviewed the GEO design documentation and verified that the system designs clearly and accurately mapped to testing requirements and included architectural and interface diagrams.

(CUI) Although the penetration testing had not been initiated at the time of our audit, we verified that the contractor plans to complete penetration testing in March 2025, which is consistent with the established test schedule. [REDACTED]

[REDACTED]

(CUI) [REDACTED]

(CUI) [REDACTED]

<sup>15</sup> (U) A denial of service is a type of cyber attack in which a malicious actor seeks to prevent authorized access to a system resource or to delay system operations and functions.

(U) CAPEC is a publicly available database of common attack patterns that help software developers and others understand how adversaries exploit weaknesses in cyber-enabled capabilities. The database contains a description of each attack pattern, how an adversary would conduct an attack, methods for mitigating an attack, and the likelihood and severity of each attack. Identifying attack patterns assists the developers to better understand the specific elements of common attack applications and systems. The DoD Technology and Program Protection Guidebook instructs programs to review the CAPEC database early in the software development process to analyze common attacks that may impact the program.<sup>16</sup>

(EU) [REDACTED]

- **(U) Trusted Identifiers** – an adversary guesses or obtains a trusted identifier to perform authorized actions under the guise of an authenticated user or service. This attack pattern can be successful if the software accepts user input without verifying its authenticity.
- **(U) Leveraging Race Conditions** – an adversary targets a race condition, which occurs when a program that is designed to manage tasks in a specific sequence is asked to perform two or more operations at the same time. The adversary can take advantage of the time lapse between when the tasks are initiated and ordered, and when the security controls take effect.
- **(U) Adversary in the Middle** – an adversary targets the communication between two components (for example, between client and server) looking for opportunities to exploit. This attack pattern can be successful when strong authentication is not used between the components or the communication occurs “in the clear,” meaning without encryption.
- **(U) Buffer Manipulation** – an adversary manipulates an application’s interaction with a buffer by identifying a programmatic means for interacting with the buffer, such as vulnerable code. A buffer is a region of memory used to store data temporarily while it is being moved from one place to another.

<sup>16</sup> (U) Office of the Under Secretary of Defense for Research and Engineering, “DoD Technology and Program Protection Guidebook,” July 2022.



- **(U) Action Spoofing** – an adversary tricks a user into initiating an action (such as clicking on a link on a website) that then downloads malicious software.
- **(U) Resource Injection** – an adversary exploits weaknesses in input validation by manipulating resource identifiers, enabling the unintended modification or specification of a resource. A resource identifier is a unique string of characters that distinguishes one resource from another, such as a Uniform Resource Locator (URL).

(~~CUI~~) [Redacted]

(~~CUI~~) [Redacted]

(~~CUI~~) [Redacted]

(~~CUI~~) [Redacted]

(EU) [REDACTED]  
[REDACTED]  
[REDACTED]<sup>17</sup>

(EU) [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

### **(U) PMO Officials Are Authorized to Tailor SwA Activities Based on Risk But the PPP Does Not Have to Reflect the Risk Acceptance**

(U) DoDI 5000.83 and the SwA Countermeasures in Program Protection Planning allow the Program Manager to tailor the program protection planning procedures, including SwA, based on the characteristics of the required capability and the associated risk. However, the risk accepted by not conducting or completing an SwA activity is not required to be detailed in the PPP, which results in an incomplete risk profile. If the MDA doesn't have a complete risk profile, they cannot make an informed decision on the program's cost, schedule, or performance, which could result in the Next Gen OPIR program transitioning to the next stage in the acquisition lifecycle prior to all system risk being identified and addressed or moving to the next stage without a full understanding of the related risks. Therefore, we recommend that the Under Secretary of Defense for Research and Engineering revise PPP guidance to include a process for the identification of software assurance risks and steps for how the acceptance of risks should be tracked, if left unmitigated.

<sup>17</sup> (U) High vulnerabilities can have a catastrophic (causing a large amount of destruction, or a violent change) adverse effect on DoD organizational operations, assets, or individuals. For example, high vulnerabilities may result in loss of classified or highly sensitive data or equipment that could impair operations affecting national interest for an indefinite period of time.

(U) For GEO satellite software, PMO officials did not ensure that the PPP was consistently updated to reflect the SwA activities conducted, and had not submitted the PPP for MDA approval since October 2020. DoDI 5000.83 requires PMOs to update PPPs throughout the weapon system life cycle and the Air Force Systems Security Engineering Cyber Guidebook requires that the PPP be updated annually. Therefore, we recommend that the Next Gen OPIR Program Manager ensure that the GEO Program Protection Lead regularly update the GEO PPP, at a minimum annually, to accurately reflect the PMO and contractor’s progress implementing SwA activities. We also recommend that the Next Gen OPIR Program Manager submit the PPP to the MDA for approval in accordance with the Air Force Systems Security Engineering Cyber Guidebook.

(CUI) [REDACTED]

(U) In February 2024, the National Science and Technology Council issued a report listing space technologies and systems as critical and emerging technologies, significant to U.S. national security.<sup>18</sup> Ensuring that the software associated with space technologies and programs, such as the Next Gen OPIR, is reliable and secure is imperative to ensuring that the systems can perform their critical missions. If PMO officials do not ensure that all SwA activities are conducted during software development, there is an increased risk that software may include vulnerabilities that could prevent the GEO satellites from performing their mission. The later in the acquisition lifecycle that vulnerabilities are identified and corrected, the costlier and more difficult it typically is to fix those vulnerabilities. Furthermore, if the PPP does not reflect the risk acceptance associated with SwA and is not reviewed and updated annually, the MDA will not be fully informed of the program risk and cannot rely on the PPP as part of their assessment to determine whether programs will meet cost, schedule, and performance milestones, or that the programs are ready to transition to the next phase of the acquisition lifecycle.

<sup>18</sup> (U) National Science and Technology Council Fast Track Action Subcommittee on Critical and Emerging Technologies, “Critical and Emerging Technologies List Update,” February 2024.

## **(U) Recommendations, Management Comments, and Our Response**

### **(U) Recommendation 1**

(U) We recommend that the Under Secretary of Defense for Research and Engineering revise program protection plan guidance to include a process for the identification of software assurance risks and steps for how the acceptance of risks should be tracked, if left unmitigated.

### **(U) Management Comments Required**

(U) The Under Secretary of Defense for Research and Engineering did not provide comments on the recommendation; therefore, the recommendation is unresolved. We request that the Under Secretary provide comments within 30 days of the final report that detail the actions taken or planned to address the recommendation.

### **(U) Recommendation 2**

(U) We recommend that the Next Generation Overhead Persistent Infrared Program Manager:

- a. (CUI) [Redacted]
- b. (CUI) [Redacted]
- c. (CUI) [Redacted]
- d. (CUI) [Redacted]

***(U) Recommendation 3***

**(U) We recommend that the Next Generation Overhead Persistent Infrared Program Manager:**

- a. **(U) Ensure that the Geosynchronous Earth Orbit Program Protection Lead regularly updates the Geosynchronous Earth Orbit program protection plan, at a minimum annually, to accurately reflect the program management office and contractor's progress implementing software assurance activities.**
- b. **(U) Submit the program protection plan to the Milestone Decision Authority for approval, in accordance with the Air Force Systems Security Engineering Cyber Guidebook.**

***(U) Management Comments Required***

(U) The Next Generation Overhead Persistent Infrared Program Manager did not provide comments on the recommendations; therefore, the recommendations are unresolved. We request that the Program Manager provide comments within 30 days of the final report that detail the actions taken or planned to address the recommendations.

## (U) Appendix

---

### (U) Scope and Methodology

(U) We conducted this performance audit from April 2023 through June 2024 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

(U) We reviewed the following policy and guidance.

- (U) DoDI 5000.83, “Technology and Program Protection to Maintain Technological Advantage,” July 20, 2020 (Change 1 Effective: May 21, 2021)
- (U) DoDI 5000.90, “Cybersecurity for Acquisition Decision Authorities and Program Managers,” December 31, 2020
- (U) DoDI 5200.44, “Protection for Mission Critical Functions to Achieve Trusted Systems and Networks (TSN),” November 5, 2012 (Incorporating Change 3, October 15, 2018)
- (U) Deputy Assistant Secretary of Defense for Systems Engineering and DoD Chief Information Officer, “Software Assurance Countermeasures in Program Protection Planning,” March 2014
- (U) Deputy Assistant Secretary of Defense for Systems Engineering, “PPP Outline and Guidance,” July 2011

(U) We acquired a universe of weapon system programs approved through Milestone B. We nonstatistically selected the Next Gen OPIR program for review based on the program’s software development progress through the DoD acquisition lifecycle at the time it was selected, and level of software-dependent components within the Next Gen OPIR system. We then obtained and analyzed Next Gen OPIR program documents including:

- (U) Next Gen OPIR Contract and Associated Modifications;
- (U) GEO PPP, Version 2.0, October 3, 2020;
- (U) GEO Software Development Plan, Revision C, November 3, 2021;
- (U) GEO CT&E Plan, DRAFT, May 30, 2022, and GEO CT&E Plan, October 11, 2023; and
- (U) Supporting documentation for SwA countermeasures such as scan results, design documents, and test schedules.

(U) We conducted a site visit to the Next Gen OPIR PMO in El Segundo, California, to gain an understanding of the program, select components for review, and learn how SwA was applied to the system. After learning about the program and components involved, we nonstatistically selected the Next Gen OPIR GEO satellites' mission payload module software to review because, at the time of our review, the Next Gen OPIR PMO and contractor software developers had completed most of the program's software development. We also met with the contractor to observe and analyze the implementation of all SwA activities applicable to the development process. The contractor (third-party stakeholder) reviewed and commented on relevant portions of the draft report and any comments provided were considered in preparing the final report.

(U) This report was reviewed by the DoD Component 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 Component about the CUI treatment of their information. If the DoD Component failed to provide any sufficient comments about the CUI treatment of their information, we marked the report based on our assessment of the available information.

### **(U) Internal Control Assessment and Compliance**

(~~EU~~) We assessed internal controls with laws and regulations necessary to satisfy the audit objective. In particular, we assessed control activities related to the Next Gen OPIR PMO's oversight and management of the Next Gen OPIR program to implement SwA countermeasures. [REDACTED]

[REDACTED]

### **(U) Use of Computer-Processed Data**

(U) We obtained and analyzed computer-processed data from static analysis scanning tools used by the Next Gen OPIR contractor. Specifically, we were provided static analysis scan results for the selected components of the Next Gen OPIR program. To determine the reliability and completeness of the computer-processed data, we interviewed the Next Gen OPIR contractor,

(U) discussed the results with them during our site visit, and reviewed standard operating procedures for the tools being used. We also verified that the contractor used a DoD-approved tool to conduct static analysis and process scan results. Based on our reviews of the scan results and verification of the tool used by the contractor, we consider the information presented in the scan results to be sufficiently reliable for the purpose of our audit.

## **(U) Use of Technical Assistance**

(U) An engineer in the Research and Engineering Division of the DoD OIG's Evaluations component provided technical assistance. The engineer helped analyze and interpret supporting documentation and results related to implemented SwA countermeasures.

## **(U) Prior Coverage**

(U) During the last 5 years, the Government Accountability Office (GAO) issued four reports related to SwA. Unrestricted GAO reports can be accessed at <https://www.gao.gov>.

## **(U) GAO**

(U) Report No. GAO-20-146, "Space Command and Control: Comprehensive Planning and Oversight Could Help DoD Acquire Critical Capabilities and Address Challenges," October 2019

(U) The GAO assessed the status of Air Force efforts to develop advanced command and control capabilities for space and identified the Air Force's challenges developing these capabilities. In the report, the GAO concluded that the program faced management issues related to technical complexity. Additionally, the GAO concluded that software integration and cybersecurity challenges existed, which further complicated program development. The report contained recommendations that the Under Secretary of Defense for Acquisition and Sustainment (USD[A&S]) ensure the Air Force's finalized program's acquisition strategy includes risk management plans, metrics for measuring quality of software, and workforce assessments. The GAO also recommended that the USD(A&S) should ensure that the Air Force's program conducts periodic independent reviews to assess the program's approach to developing software.



(U) Report No. GAO-22-105230, "Weapon Systems Annual Assessment: Challenges to Fielding Capabilities Faster Persist," June 2022

(U) The GAO analyzed 63 of the DoD's costliest weapon system acquisition programs to determine each program's characteristics and performance, implementation of knowledge-based acquisition practices, modern software development approaches, and cybersecurity practices. In the report, the GAO concluded that major defense acquisition programs (MDAPs) continue to struggle with schedule delays. Over half of the 29 MDAPs that the GAO reviewed, that had yet to deliver capability, reported delays during the past year. The lack of future year funding data in the FY 2022 budget request precluded the GAO from assessing the MDAP portfolio's cost performance in 2022. The report contained recommendations that the DoD update its industrial base assessment instruction to define the circumstances that would constitute a known or projected problem or substantial risk that a necessary industrial capability may be lost.

(U) Report No. GAO-19-136, "DoD Space Acquisitions: Including Users Early and Often in Software Development Could Benefit Programs," March 2019

(U) The GAO reviewed four software-intensive major defense programs with cost growth or schedule delays attributed, in part, to software development challenges. In the report, the GAO concluded that the DoD struggled to deliver software-intensive space programs that meet operational requirements within expected time frames. Although user involvement is critical to the success of any software development effort, key programs often did not effectively engage users. Program efforts to involve users and incorporate feedback frequently did not match plans. In the report, the GAO concluded that this was due to the lack of specific guidance on the timing, frequency, and documentation for user involvement and feedback. The lack of user engagement has contributed to systems that were later found to be operationally unsuitable. The report contained recommendations that the DoD ensure its guidance that addresses software development provides specific, required direction on the timing, frequency, and documentation of user involvement and feedback.

(U) Report No. GAO-19-128, “Weapon System Cybersecurity: DoD Just Beginning to Grapple with Scale of Vulnerabilities,” October 2018

(U) The GAO addressed, at the request of Congress, factors that contribute to the current state of DoD weapon systems cybersecurity, vulnerabilities in weapons that are under development, and steps the DoD is taking to develop more cyber-resilient weapon systems. In the report, the GAO concluded that multiple factors contribute to the current state of DoD weapon systems cybersecurity, including the increasingly computerized and networked nature of DoD weapons, the DoD’s past failure to prioritize weapon systems cybersecurity, and the DoD’s emerging understanding of how best to develop more cyber-secure weapon systems. The GAO concluded that the DoD did not prioritize cybersecurity in weapon systems acquisitions, partly because the DoD historically focused on the cybersecurity of its networks, but not weapon systems themselves. The DoD is in the early stage of understanding how to apply cybersecurity to weapon systems. Therefore, the report concluded that the GAO would continue to evaluate this issue.

## **(U) Acronyms and Abbreviations**

---

<b>AFRL</b>	Air Force Research Lab
<b>CAPEC</b>	Common Attack Pattern Enumeration and Classification
<b>CT&amp;E</b>	Cyber Test and Evaluation
<b>CVE</b>	Common Vulnerabilities and Exposures
<b>CWE</b>	Common Weakness Enumeration
<b>DoDI</b>	Department of Defense Instruction
<b>GAO</b>	Government Accountability Office
<b>GEO</b>	Geosynchronous Earth Orbit
<b>MDA</b>	Milestone Decision Authority
<b>MPL</b>	Mission Payload
<b>Next Gen OPIR</b>	Next Generation Overhead Persistent Infrared
<b>PMO</b>	Program Management Office
<b>PPP</b>	Program Protection Plan
<b>SwA</b>	Software Assurance



## **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 [www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/](http://www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/) or contact the Whistleblower Protection Coordinator at [Whistleblowerprotectioncoordinator@dodig.mil](mailto: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](mailto:public.affairs@dodig.mil); 703.604.8324



[www.twitter.com/DoD\\_IG](http://www.twitter.com/DoD_IG)

### **LinkedIn**

[www.linkedin.com/company/dod-inspector-general/](http://www.linkedin.com/company/dod-inspector-general/)

### **DoD Hotline**

[www.dodig.mil/hotline](http://www.dodig.mil/hotline)



**CUI//SP CTI**



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

4800 Mark Center Drive  
Alexandria, Virginia 22350-1500  
[www.dodig.mil](http://www.dodig.mil)  
DoD Hotline 1.800.424.9098

**CUI//SP CTI**