Report No. DODIG-2025-165

~~CUI~~

INSPECTOR GENERAL

U.S. Department of Defense

SEPTEMBER 23, 2025

(U) Management Advisory: The National Information Assurance Partnership's Evaluation and Certification Process for Commercial Off-the-Shelf Products

~~Controlled by: DoD OIG~~
~~Controlled by: Audit, Cyberspace Operations~~
~~CUI Category: ISVI~~
~~Distribution/Dissemination Control: NOFORN~~
~~POC:~~ [redacted]

INDEPENDENCE ★ INTEGRITY ★ EXCELLENCE ★ TRANSPARENCY

~~CUI~~


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

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

September 23, 2025

MEMORANDUM FOR CYBERSECURITY DIRECTOR, NATIONAL SECURITY AGENCY
DIRECTOR, NATIONAL INFORMATION ASSURANCE PARTNERSHIP

SUBJECT: (U) Management Advisory: The National Information Assurance Partnership's Evaluation and Certification Process for Commercial Off-the-Shelf Products (Report No. DODIG-2025-165)

(U) The purpose of this management advisory is to inform responsible DoD officials of concerns identified during the DoD Office of Inspector General's "Audit of the DoD's Actions to Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities," announced on March 11, 2024. These concerns relate to the National Information Assurance Partnership's process for evaluating and certifying commercial off-the-shelf products.

(U) We prepared this advisory in accordance with generally accepted government auditing standards except for the requirement to include a detailed methodology, which we omitted for conciseness. Those standards require that we plan and perform the project to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our project objective. Although we did not comply with all generally accepted government auditing standards, we believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our project objective. Further details about the methodology are available on request.

(U) We provided copies of the draft management advisory to the National Information Assurance Partnership Director and the National Security Agency Cybersecurity Director and requested written comments on the recommendations. We considered management's comments on the draft when preparing the final management advisory. These comments are included in the management advisory.

(U) This management advisory contains six recommendations. We consider one recommendation closed because the Acting National Security Agency Cybersecurity Director took action sufficient to address the recommendation, one recommendation unresolved because the Acting National Security Agency Cybersecurity Director did not fully address the recommendation presented in the report, and four recommendations resolved but open. We will track the unresolved recommendations until management has agreed to take actions that we determine to be sufficient to meet the intent of the recommendations. We will close the recommendations when management officials submit documentation showing that all agreed-upon actions to implement them are completed.

(U) DoD Instruction 7650.03 requires that recommendations be resolved promptly. For the unresolved recommendations, please provide us within 30 days your response concerning specific actions in process or alternative corrective actions proposed on the recommendations. Send your responses to either [redacted] if unclassified or

(U) [redacted] if classified SECRET. For the resolved recommendations, please provide us documentation within 90 days showing you have completed the agreed-upon actions. Send your response as a PDF file to either [redacted] if unclassified or [redacted] if classified SECRET. Responses must have the actual signature of the authorizing official for your organization.

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

Sean J. Keaney
Acting Assistant Inspector General for Audit
Cyberspace Operations

(U) Recommendations Table

(U) Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Director, National Information Assurance Partnership	1.c	1.a.1, 1.a.2, 1.b, 1.d.2	1.d.1 **(U)**

(U) Please provide Management Comments by October 24, 2025.

(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.


INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
INTEGRITY
EFFICIENCY

(U) Introduction

(U) On March 11, 2024, we announced the "Audit of the DoD's Actions to Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities," (Project No. D2024-D000CU-0099.000).[1] The objective of the audit was to determine whether the actions taken by DoD Components to identify, respond to, and mitigate vulnerabilities impacting Ivanti Connect Secure (ICS) and Ivanti Policy Secure (IPS) complied with DoD requirements.[2] During the audit, we identified concerns with the National Information Assurance Partnership's (NIAP) process for evaluating and certifying commercial off-the-shelf (COTS) information technology (IT) products for use on national security systems (NSS).[3] This management advisory focuses on that process and provides recommendations for corrective action.

(U) Background

(U) The National Security Agency (NSA) manages and operates NIAP, which oversees the U.S. program to evaluate COTS IT products against international security requirements, referred to as the "Common Criteria." As of July 2025, 35 nations were part of the Common Criteria Recognition Arrangement, which promotes mutual recognition of certified COTS IT products. NIAP is responsible for overseeing the evaluations of the COTS IT products, which are performed by Common Criteria Testing Laboratories (CCTLs); validating that the results of the evaluations are correct and compliant with NIAP policies; and certifying the products that successfully complete the evaluation.[4] Once NIAP certifies the products, it adds them to its Product Compliant List (PCL) and the Common Criteria Certified Products List.

(U) Although any organization may select COTS IT products for use from the PCL, Committee on National Security Systems Policy (CNSSP) No. 11 states that all COTS IT products acquired for use on NSS must comply with NIAP requirements.[5] Specifically, CNSSP No. 11 requires the heads of U.S. Government departments and agencies to select COTS IT products from the NIAP PCL to protect NSS and the information that resides on them.

---

[1] (U) This management advisory contains information that has been redacted because the DoD identified it as Controlled Unclassified Information that is not releasable to the public. Controlled Unclassified Information 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.

[2] (U) Ivanti, Inc. provides information technology management and software solutions, including virtual private networks, such as ICS, which allows users to remotely connect to a network over the Internet through a secure tunnel. IPS is a network access control solution composed of hardware and software that is designed to provide network access to only authorized users and devices.

[3] (U) COTS refers to software and hardware products that are commercially ready-made and available for sale, lease, or license to the public. An NSS is any information system used or operated by an agency or contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications); or (ii) is protected at all times by procedures established for information specifically authorized under criteria established by an executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

[4] (U) CCTLs are commercial testing laboratories accredited by the National Institute of Standards and Technology through the National Voluntary Accreditation Program and approved by NIAP to perform security evaluations of COTS IT products.

[5] (U) CNSSP No. 11, "National Policy Governing the Acquisition of Cybersecurity and Cybersecurity-Enabled IT Products and Services," February 28, 2025.

(U) NIAP Evaluation and Certification Process

(U) The NIAP evaluation and certification process begins when a COTS IT product vendor selects one of the nine CCTLs to evaluate the product against one or more protection profiles approved by NIAP and the Common Criteria Recognition Arrangement. A protection profile is a baseline set of security requirements for a specific category of technology that must be in place to mitigate security threats regardless of the intended product use. For example, protection profiles exist for virtual private network (VPN) solutions, network devices, and operating systems and specify the security requirements for each type of product.[6]

(U) According to NIAP officials, the vendors work closely with the CCTLs to select which product features will be tested, determine the protection profiles to test against, and draft a security target.[7] NIAP does not require that the CCTL test all features of a product. For example, if a product has multiple uses, such as a network device that is also a VPN, the vendor and CCTL can choose to test only one use and not the other.

(U) After the vendor and CCTL select the protection profile and develop the security target, the CCTL evaluates the product, which includes verifying that the product's security features adhere to the protection profile and analyzing the product for vulnerabilities to identify potential weaknesses. The vulnerability assessment includes searching public records for vulnerabilities identified with the product and testing for known vulnerabilities. After the CCTL completes its evaluation, it drafts an "Assurance Activity Report" and submits the report to NIAP for validation.[8] NIAP officials validate the results by reviewing the evaluation report and supporting documentation for technical accuracy and completeness before certifying the product.[9] If NIAP certifies the product, the product is added to the NIAP PCL and the Common Criteria Certified Products List. Figure 1 shows an overview of the NIAP evaluation and certification process.

---

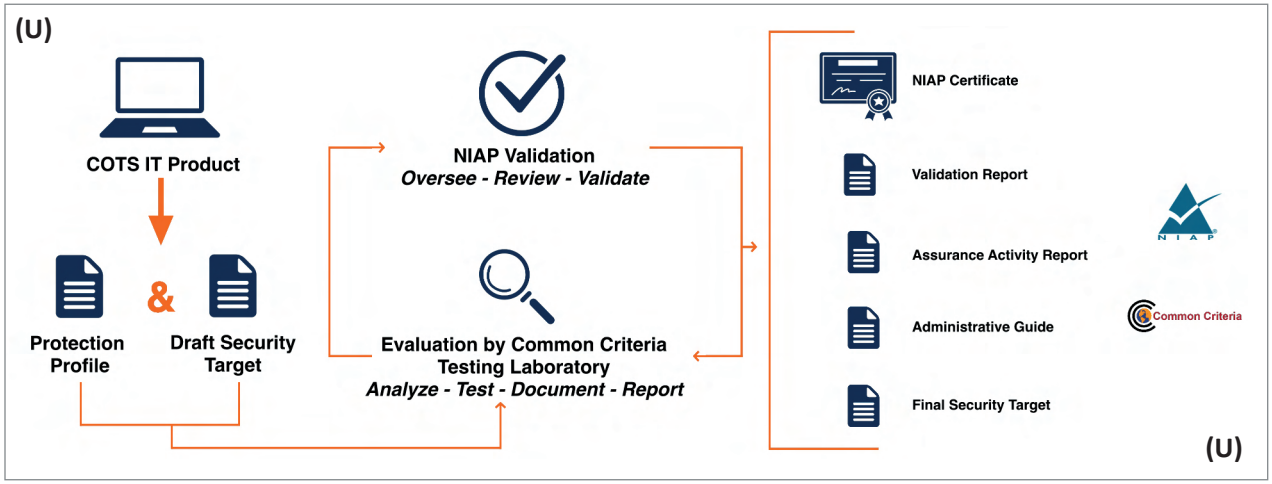
[6] (U) A network device is a device that is connected to a network and has a role in the underlying system or foundation of the network, for example a router, firewall, VPN, or intrusion detection system.

[7] (U) A security target is a statement of the security requirements specific to the product being evaluated.

[8] (U) For this management advisory, we will refer to the CCTL's "Assurance Activity Report" as the evaluation report.

[9] (U) NIAP officials also draft a "Validation Report" that summarizes the evaluation results and confirms that the overall results are acceptable. In addition, the CCTL drafts "Administrative Guidance" with instructions to users on how to configure the COTS IT product to comply with the evaluated configuration.

(U) Figure 1. NIAP Evaluation and Certification Process



(U) Source: NIAP.

(U) NIAP Policies and Guidance

(U) NIAP Policy Letter #17 states that NIAP will not certify a product with known security-related vulnerabilities.[10] Policy Letter #17 also states that if a vulnerability is discovered before, during, or after an evaluation, NIAP may notify the product vendor and require modifications for the product to be included on the PCL. Additionally, the Policy Letter requires vendors to notify NIAP if the vendor discovers or is made aware of a vulnerability associated with a product on the PCL.

(U) NIAP Policy Letter #26 requires that products evaluated by NIAP for use on NSS cannot be otherwise prohibited from use on NSS by statute, executive order, or any other directives applicable to NSS owners.[11] In addition, Policy Letter #26 states that NIAP reserves the right to refuse evaluation and certification of a product if it will soon be prohibited for use on NSS or has already been prohibited from a class of NSS.

(U) NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) Publication #2 states that the NIAP Director will withdraw a NIAP-issued certification if evidence conclusively demonstrates the product no longer meets the criteria for which it was evaluated.[12] CCEVS Publication #3 states that NIAP officials will validate the CCTL's evaluation results and conclusions to confirm the technical quality, correctness, and consistency of each evaluation in accordance with all NIAP guidance.[13]

[10] (U) NIAP Policy Letter #17, "Effects of Vulnerabilities in Evaluated Products," August 29, 2014. This policy was updated on May 1, 2025. NIAP issues Policy Letters to provide operational guidance and Common Criteria Evaluation and Validation Scheme Publications to provide guidance for completing product evaluations.

[11] (U) NIAP Policy Letter #26, "Limitation to Acceptance of a Product for NIAP Evaluation and Posting on the NIAP PCL," March 20, 2019.

[12] (U) NIAP CCEVS Publication #2, "Quality Manual and Standard Operating Procedures," January 2020.

[13] (U) NIAP CCEVS Publication #3, "Guidance to Validators," February 2020.

~~(CUI)~~ NIAP Certified ICS and IPS After Ivanti Disclosed Vulnerabilities and the NSA Issued a [redacted]

~~(CUI)~~ On February 23, 2024, NIAP certified ICS and IPS and added them to the PCL after Ivanti disclosed vulnerabilities affecting the products that were not analyzed by the CCTL and the NSA [redacted] This occurred because the NIAP evaluation and certification process did not require NIAP officials to take the following steps before certifying a COTS IT product and adding it to the PCL.

- (U) Conduct a search of public records and vendor websites to identify any vulnerabilities disclosed after the date of the CCTL's public records search and have the CCTLs conduct additional testing, if warranted.
- (U) Identify any statutes, executive orders, or other directives prohibiting use of the COTS IT product on NSS.

(U) In addition, NIAP officials did not require testing of the core features of COTS IT products, including ICS and IPS, or clearly disclose on the PCL which features were tested and certified for use on NSS and which were not. Instead, NIAP listed the products on the PCL without clear notification to NSS owners that the products included unevaluated features.

~~(CUI)~~ On May 14, 2024, we notified NIAP officials of the additional ICS and IPS vulnerabilities and the NSA [redacted]; however, as of July 30, 2025, NIAP had not removed the products from the PCL.[14] NSA officials overseeing NIAP stated that NIAP lacked a policy allowing it to remove products from the PCL when additional vulnerabilities had been identified. NSS owners rely on the NIAP PCL to procure COTS IT products that have been evaluated and certified for use on NSS. Because NIAP included products on the PCL that should not have been certified, such as ICS and IPS, and did not clearly identify the specific features of the products that were evaluated and certified, NSS owners could select and install vulnerable products on their NSS or unknowingly use untested features of products, putting highly sensitive national security information at risk of compromise.

[14] (U) We issued the draft version of this report on July 30, 2025.

(U) ICS and IPS Vulnerability Disclosures and Federal Response

(U) On January 10, 2024, Ivanti publicly disclosed one highly severe and one critically severe zero-day cybersecurity vulnerability affecting its ICS and IPS products.[15] According to Mandiant, a U.S. cybersecurity firm, malicious actors could exploit the vulnerabilities to bypass authentication controls, steal user credentials, gain unauthorized access to a network, and leave a file behind to establish persistent, long-term access. Ivanti disclosed three additional highly severe vulnerabilities affecting ICS and IPS between January 31, 2024, and February 8, 2024.

~~(CUI)~~ In response to Ivanti's vulnerabilities disclosure, multiple Federal agencies, including the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and the NSA, issued security advisories, emergency directives (EDs), supplemental directions, and orders to mitigate the vulnerabilities. On January 19, 2024, CISA issued an ED directing Federal civilian Executive Branch agencies to immediately mitigate the vulnerabilities affecting ICS and IPS.[16] The ED stated that CISA determined that exploitation of the vulnerabilities and high potential for compromise posed an unacceptable risk to Federal agencies. On January 29, 2024, the NSA determined that [redacted] and issued an ED [redacted][17]

(U) NIAP Certification of ICS and IPS

~~(CUI)~~ On February 23, 2024, NIAP certified ICS and IPS and added them to the PCL after Ivanti disclosed a vulnerability that was not analyzed by the CCTL and the NSA [redacted] NIAP Policy Letter #17 states that NIAP will not certify a COTS IT product with known security vulnerabilities, and NIAP Policy Letter #26 states that COTS IT products evaluated under NIAP for use on NSS may include only those products that are not otherwise prohibited from use on NSS by statute, executive order, or other directive applicable to NSS owners. Figure 2 shows the timeline of Ivanti's vulnerability disclosures, the Federal response, and NIAP's certification and addition of ICS and IPS to the PCL.

---

15 (U) A zero-day vulnerability is a previously unknown vulnerability in an application or operating system for which there is no defense or patch. A patch is an update released by a software manufacturer to fix bugs in existing programs. The National Institute of Standards and Technology oversees the National Vulnerability Database, which provides information about individual vulnerabilities. The Common Vulnerability Scoring System produces a numerical score that reflects the severity for each vulnerability. The Database translates the score into a qualitative representation (such as low, medium, high, and critical) to help organizations assess and prioritize their vulnerability management processes.

16 (U) CISA ED 24-01, "Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities," January 19, 2024.

17 ~~(CUI)~~ NSA ED 2024-002, [redacted] January 29, 2024.

(U) Figure 2. Timeline of Ivanti Vulnerability Disclosures, Federal Response, and NIAP Certification of ICS and IPS

~~(CUI)~~

(U) Oct. 5-6, 2023	(U) CCTL conducted public domain vulnerability searches for ICS and IPS.	(U) CISA determined that the Ivanti vulnerabilities posed an unacceptable risk to Federal agencies based on their widespread exploitation, prevalence of the affected products in the Federal enterprise, high potential for compromise of agency information systems, impact of a successful compromise, and complexity of the proposed mitigations.
(U) Dec. 15, 2023	(U) CCTL completed the product evaluation reports for ICS and IPS.	
(U) Jan. 10, 2024	(U) Ivanti disclosed two common vulnerabilities and exposures (CVEs)—highly severe CVE-2023-46805 and critically severe zero-day CVE-2024-21887—affecting ICS and IPS.[1]	
(U) Jan. 19, 2024	(U) CISA issued ED 24-01 directing Federal civilian Executive Branch agencies to immediately mitigate the vulnerabilities impacting ICS and IPS.	
(U) Jan. 29, 2024	~~(CUI)~~ The NSA issued an ED [redacted]	~~(CUI)~~ The NSA issued the ED [redacted]
(U) Jan. 31, 2024	(U) Ivanti disclosed two additional highly severe vulnerabilities—CVE-2024-21888 and CVE-2024-21893—affecting ICS and IPS and released a patch for ICS.	
(U) Jan. 31, 2024	(U) CISA issued Supplemental Direction V1 directing Federal agencies to disconnect all ICS and IPS from their networks, apply mitigations before reconnecting, and threat hunt on any systems connected to—or recently connected to—the affected Ivanti products.[2]	(U) CISA updated Supplemental Direction V1 on Feb. 5, 2024, stating that malicious actors continued to leverage the vulnerabilities to compromise enterprise networks and that some have developed workarounds to earlier mitigations and detection methods.
(U) Feb. 1, 2024	(U) Ivanti released patches for ICS and IPS.	
(U) Feb. 6, 2024	(U) CCTL conducted an additional public domain vulnerability search and updated the product evaluation reports for ICS and IPS.	
(U) Feb. 8, 2024	(U) Ivanti disclosed an additional highly severe vulnerability—CVE-2024-22024—affecting ICS and IPS and released patches for ICS and IPS.	
(U) Feb. 9, 2024	(U) CISA issued Supplemental Direction V2 stating that Ivanti reported a new CVE and directing Federal agencies to apply additional mitigations to ICS and IPS and threat hunt on any systems connected to—or recently connected to—the affected Ivanti products.[3]	(U) CISA updated Supplemental Direction V2 on Mar. 4, 2024, stating that continued operation of ICS and IPS devices carried significant risk of malicious actors accessing and persisting on the devices.
(U) Feb. 14, 2024	(U) Ivanti released patches for ICS and IPS.	
(U) Feb. 23, 2024	**(U) NIAP validated, certified, and added ICS and IPS to the PCL.**	

~~(CUI)~~

[1] (U) CVEs are a standard way of identifying, defining, and cataloging publicly disclosed cybersecurity vulnerabilities. CVEs are published on the CVE.org website and available for download or search as part of the CVE Program that is operated by the MITRE Corporation and sponsored by CISA.

[2] (U) CISA Supplemental Direction V1: ED 24-01, "Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities," January 31, 2024 (Updated February 5, 2024).

[3] (U) CISA Supplemental Direction V2: ED 24-01, "Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities," February 9, 2024 (Updated March 4, 2024).

(U) Source: The DoD OIG.

(U) NIAP Evaluation and Certification Process Did Not Require Identification of Post-Evaluation Vulnerabilities or Directives

(U) The NIAP evaluation and certification process did not require NIAP officials to take the following steps before certifying a COTS IT product and adding it to the PCL.

- (U) Conduct a search of public records and vendor websites to identify any vulnerabilities disclosed after the date of the CCTL's public records search for vulnerabilities and have the CCTLs conduct additional testing, if warranted.
- (U) Identify any statutes, executive orders, or other directives prohibiting use of the COTS IT product on NSS.

(U) NIAP Was Not Required to Identify Post-Evaluation Vulnerabilities

(U) The NIAP certification process did not require NIAP officials to conduct a search of public records and vendor websites to identify vulnerabilities disclosed after the date of the CCTL's last public records search and have the CCTLs conduct additional testing, if warranted. The CCTL conducted a public records vulnerability search on October 5 and 6, 2023, for ICS and IPS, respectively. The CCTL then completed the IPS and ICS evaluation reports on December 15, 2023. Between December 15, 2023, and February 1, 2024, Ivanti disclosed four vulnerabilities affecting ICS and IPS and released two patches to mitigate the vulnerabilities.

(U) On February 5, 2024, CISA reported that malicious actors continued to exploit the initial vulnerabilities and were able to evade Ivanti's earlier mitigation efforts, including patches. On February 6, 2024, after NIAP received the CISA ED and notified the CCTL about the initial vulnerabilities reported by Ivanti, the CCTL conducted an additional public records vulnerability search and limited retesting of both ICS and IPS with the patches installed. Two days later, on February 8, 2024, Ivanti disclosed the fifth vulnerability affecting ICS and IPS. On February 8 and 14, 2024, Ivanti released replacement patches to address the ongoing exploitation of vulnerabilities.

(U) On February 23, 2024, NIAP officials reviewed and validated the CCTL's evaluation reports of ICS and IPS. NIAP officials stated that they certified ICS and IPS based on the CCTL report stating that Ivanti patched the vulnerabilities. NIAP officials stated that they were unaware that Ivanti had disclosed a fifth vulnerability before they certified ICS and IPS or that Ivanti released replacement patches because malicious actors continued to actively exploit the vulnerabilities. Therefore, we recommend that the NIAP Director, in coordination with the NSA Cybersecurity Director, revise the product evaluation process to require NIAP officials to conduct a search of public records for vulnerabilities disclosed after the CCTL's last vulnerability search and, if a new vulnerability is discovered, return the product to the CCTL for additional testing before certifying a product for inclusion on the PCL.

(U) According to the CCTL evaluation reports for ICS and IPS, the CCTLs reviewed the following four sources when conducting their evaluation of the COTS IT products—the National Vulnerability Database, documentation for one of the software components required to use the products, the Ivanti website, and an Ivanti forums website about two previous vulnerabilities from 2023. Although those sources included technical vulnerability information, the publicly available CISA website provides more contextual, detailed, and regularly updated information, including how malicious actors are actively exploiting the vulnerabilities, what malicious actors could do after compromising a system, the prevalence of exploitation, and the degree of risk the vulnerabilities pose to Federal agencies. On May 1, 2025, NIAP officials revised Policy Letter #17 and included an addendum with guidance for mitigating vulnerabilities before certification. Specifically, the addendum requires CCTLs to search the CISA website for product and vulnerability information as part of the vulnerability assessment. Therefore, we are not making a recommendation to include the CISA website among the required sources searched for vulnerability information.

(U) NIAP Was Not Required to Identify Directives Applicable to NSS

~~(CUI)~~ The NIAP certification process did not require NIAP to identify statutes, executive orders, or other directives prohibiting use of the COTS IT product on NSS. On January 29, 2024, while ICS and IPS were still under evaluation, the NSA issued an ED stating that the [redacted] because of the two actively exploited zero-day vulnerabilities affecting ICS and IPS. The ED stated that successful exploitation of these vulnerabilities allowed a malicious actor to move laterally between networks, exfiltrate data, and establish persistent access, resulting in full compromise of an IT system. To mitigate the risk to NSS, the NSA [redacted][18]

(U) Although Policy Letter #26 states that NIAP may only evaluate COTS IT products that are not otherwise prohibited from use on NSS by statute, executive order, or other directive applicable to NSS owners and NSA officials stated that NIAP officials had access to the distribution portal for all NSA directives, there is no requirement for NIAP to identify any directive associated with the product before certification. Therefore, we recommend that the NIAP Director, in coordination with the NSA Cybersecurity Director, revise the product evaluation process to require NIAP officials to conduct a review of statutes, executive orders, and other directives applicable to NSS owners, including NSA directives, to determine whether the product has been prohibited from use before certifying a product for inclusion on the PCL.

[18] (U) As of August 2025, the NSA has not rescinded the ED nor released any further guidance regarding ICS and IPS.

(U) NIAP Did Not Require Testing of Core Features or Distinguish the Certified Product Features on the PCL

(U) NIAP officials did not require Ivanti to select a protection profile that tested the core features of ICS and IPS or clearly distinguish which features of a product were tested and certified for use on NSS and which were not. For example, Ivanti chose to test ICS, which is marketed as a VPN, against the network device protection profile and not the VPN protection profile.[19] As a result, NIAP certification for ICS was not based on testing of the VPN, which was the core feature of ICS and available to users. In February 2025, after we brought this issue to their attention, NIAP officials revised Policy Letter #12 to require vendors to select a protection profile that includes the core feature of the product being evaluated. The policy revision should ensure that the product's intended marketing use or purpose is tested during the evaluation process. Therefore, we are not making a recommendation to address the selection of protection profiles.

(U) NIAP also did not distinguish on the PCL which features of a COTS IT product were tested and which were not.[20] NIAP officials stated that NSS owners were responsible for using only certified features of a product and should review the protection profile documentation for the products on the PCL. However, the PCL website did not clearly state whether all the product's features were tested, leaving NSS owners to individually analyze extensive evaluation documentation to determine which features are prohibited from use on NSS. In addition to the inefficiencies associated with conducting individual analysis, some NSS owners may not be aware that such analysis is necessary. As a result, NSS owners may introduce unnecessary risks to their critical systems by using a COTS IT product's untested, noncertified core features. Therefore, we recommend that the NIAP Director, in coordination with the NSA Cybersecurity Director, revise the NIAP PCL website to include, at a minimum, the core features, the full name of the protection profiles, a list of features that have been tested and certified for use on NSS, and a list of features that have not been tested and not certified for use on NSS for each product on the PCL.

(U) NIAP Did Not Remove ICS and IPS from the PCL

~~(CUI)~~ NIAP officials were notified of the ICS and IPS vulnerabilities and NSA [redacted] on May 14, 2024; however, they had not removed the products from the PCL as of July 30, 2025. According to NSA officials, NIAP lacks the policy necessary to remove COTS IT products from the PCL once certified. However, CCEVS Publication #2 states that the NIAP Director will withdraw a NIAP-issued certification if evidence conclusively demonstrates the

[19] (U) More than 97 percent of products classified as VPNs on the PCL were evaluated against a VPN protection profile and at least one other protection profile.

[20] (U) The PCL includes the identification number, vendor name, product name, CCTL, abbreviated name of the protection profile, certification status and date, certification maintenance date and link to maintenance documentation (if any), and the certifying country. Some additional information about the product and evaluation and links to the administrative guide, evaluation report, validation report, security target, and certificate are available on the "Full Details" page of each product.

~~(CUI)~~ product no longer meets the criteria for which it was evaluated. The lack of comprehensive vulnerability testing and the NSA [redacted] are adequate reasons for withdrawing NIAP certification for ICS and IPS and without NIAP certification, ICS and IPS should also be removed from the PCL. Therefore, we recommend that the NIAP Director, in coordination with the NSA Cybersecurity Director, immediately remove IPS and ICS from the PCL.

(U) Federal agencies rely on the NIAP PCL for procuring COTS IT products that have been tested and certified for use on NSS. When a certified product is affected by a vulnerability so serious as to invoke an ED that requires agencies to immediately and indefinitely disconnect products from their NSS, immediate action by NIAP is also required. If NIAP does not take immediate action and remove vulnerable products from the PCL, NSS owners may not be aware that a certified COTS IT product has been prohibited for use on NSS, putting national security information at risk. During the audit, NIAP officials revised Policy Letter #17 to allow them to remove a product from the PCL without notice if: (1) the vendor does not notify NIAP of a vulnerability associated with a product listed on the PCL, or (2) NIAP receives mandated national guidance, such as a statute or directive from the National Manager for NSS, that would require removing a product from the PCL. However, the revision to Policy Letter #17 allows NIAP to remove products without notice only under those two scenarios, preventing NIAP from quickly removing products that violate NIAP policies or pose a substantial risk to NSS. Therefore, we recommend that the NIAP Director, in coordination with the NSA Cybersecurity Director, develop and implement policy and procedures for NIAP to quickly suspend or remove certified products from the PCL when they no longer meet the requirements for NIAP certification, violate any NIAP policy, or pose a substantial risk to NSS and disclose that a product has been suspended or removed, including the reasoning for the suspension or removal, on the PCL website.

(U) NSS Owners Could Unknowingly Put NSS at Increased Cybersecurity Risk

(U) Including COTS IT products on the PCL that should not have been certified and not distinguishing the specific features of products that were evaluated and certified could result in NSS owners installing vulnerable products on their NSS. By installing vulnerable COTS IT products, NSS owners could put highly sensitive national security information at risk of compromise. For example, CISA disclosed in March 2024 that two of its systems were compromised by malicious actors exploiting the Ivanti vulnerabilities.

(U) Recommendations, Management Comments, and Our Response

(U) Recommendation 1

(U) We recommend that the National Information Assurance Partnership Director, in coordination with the National Security Agency Cybersecurity Director:

a. (U) Revise the product evaluation process to:

1. (U) Require National Information Assurance Partnership officials to conduct a search of public records for any vulnerabilities disclosed after the Common Criteria Testing Laboratory's last vulnerability search and, if a new vulnerability is discovered, return the product to the Common Criteria Testing Laboratory for additional testing before certifying a product for inclusion on the Product Compliant List.

(U) National Information Assurance Partnership Comments

(U) The Acting National Security Agency Cybersecurity Director, responding for the National Information Assurance Partnership Director, agreed, stating that NIAP will implement a procedure to conduct a search of public records for vulnerabilities disclosed after the CCTL's last vulnerability search, and any vulnerabilities found will be resolved with the CCTL before posting products on the PCL. The Acting Director stated that NIAP will implement the procedure by September 30, 2025.

(U) Our Response

(U) Comments from the Acting Director addressed all specifics of the recommendation; therefore, it is resolved but open. We will close the recommendation once the Acting Director provides documentation verifying that NIAP revised the product evaluation process to require NIAP to conduct a search of public records for vulnerabilities disclosed after the CCTL's last vulnerability search and resolve any vulnerabilities found with the CCTL before posting products to the PCL.

2. (U) Require National Information Assurance Partnership officials to conduct a review of statutes, executive orders, and other directives applicable to National Security System owners, including National Security Agency directives, to determine whether the product has been prohibited from use before certifying a product for inclusion on the Product Compliant List.

(U) National Information Assurance Partnership Comments

(U) The Acting National Security Agency Cybersecurity Director, responding for the National Information Assurance Partnership Director, agreed, stating that effective immediately, NIAP

(U) will conduct a review of statutes, executive orders, and other directives applicable to NSS owners, including NSA directives, to determine whether a product has been prohibited from use before certifying the product for inclusion on the PCL.

(U) Our Response

(U) Comments from the Acting Director addressed all specifics of the recommendation; therefore, it is resolved but open. We will close the recommendation once the Acting Director provides documentation verifying that NIAP revised the product certification process to require NIAP to conduct a review of statutes, executive orders, and other directives applicable to NSS owners.

b. (U) Revise the National Information Assurance Partnership Product Compliant List website to include, at a minimum:

- **(U) the core features for each product,**
- **(U) the full name of the protection profiles for each product,**
- **(U) a list of features of each product that have been tested and certified for use on National Security Systems, and**
- **(U) a list of features of each product that have not been tested and not certified for use on National Security Systems.**

(U) National Information Assurance Partnership Comments

(U) The Acting National Security Agency Cybersecurity Director, responding for the National Information Assurance Partnership Director, agreed, stating that NIAP will revise the PCL website to provide system owners a clearer user interface to include the core features for each product, the full name of the protection profile, a list of features tested and certified, and a list of features not tested and not certified for use on NSS by February 2026.

(U) Our Response

(U) Comments from the Acting Director addressed the specifics of the recommendation; therefore, it is resolved but open. We will close the recommendation once the Acting Director provides documentation verifying that NIAP revised the PCL website to include the core features for each product, the full name of the protection profile, a list of features tested and certified, and a list of features not tested and not certified for use on NSS.

c. (U) Immediately remove Ivanti Policy Secure and Ivanti Connect Secure from the Product Compliant List.

(U) National Information Assurance Partnership Comments

(U) The Acting National Security Agency Cybersecurity Director, responding for the National Information Assurance Partnership Director, agreed, stating that NIAP has removed IPS and ICS from the PCL.

(U) Our Response

(U) Although the Acting Director agreed with the recommendation and stated that NIAP removed IPS and ICS from the PCL, we identified that not all versions were removed. Specifically, we verified that NIAP removed ICS version 22.2 and IPS version 22.2, which were certified on February 23, 2024, from the PCL; however, NIAP did not remove ICS version 22.7R2 and IPS version 22.7R1, which were certified on June 27, 2025, from the PCL. Therefore, we request that the Acting Director provide additional comments within 30 days of the final management advisory that address the removal of all remaining ICS and IPS versions from the PCL.

d. (U) Develop and implement policy and procedures to:

1. (U) Allow the National Information Assurance Partnership to quickly suspend or remove certified products from the Product Compliant List when they no longer meet the requirements for National Information Assurance Partnership certification, violate any National Information Assurance Partnership policy, or pose a substantial risk to national security systems.

(U) National Information Assurance Partnership Comments

(U) The Acting National Security Agency Cybersecurity Director agreed, stating that on July 29, 2025, NIAP published Policy Letter #26 to clarify the applicability and relationship of U.S. laws, regulations, and directives to product acceptance into NIAP and inclusion on the NIAP PCL. The Acting Director stated that the policy allows for the removal of a previously certified product that is prohibited from use on NSS by statute, executive order, or other directives applicable to NSS owners or operators, or the U.S. Government.

(U) Our Response

(U) Comments from the Acting Director addressed all specifics of the recommendation. We verified that NIAP published revisions to Policy Letter #26 on July 29, 2025, that allow NIAP to withdraw a product's previously issued certificate and remove it from the PCL for the protection of NSS. Therefore, the recommendation is closed.

2. **(U) Require National Information Assurance Partnership officials to disclose that a product has been suspended or removed, including the reason for the suspension or removal, on the Product Compliant List website.**

(U) National Information Assurance Partnership Comments

(U) The Acting National Security Agency Cybersecurity Director agreed, stating that NIAP will implement a procedure to post the announcement of a product's removal with reference to the appropriate national directive to the website by August 31, 2025.

(U) Our Response

(U) Comments from the Acting Director addressed all specifics of the recommendation; therefore, it is resolved but open. We will close the recommendation once the Acting Director provides documentation verifying that NIAP developed and implemented a procedure to post announcements to the PCL website concerning the products that have been removed from the PCL and the reason for their removal.

(U) Management Comments

(U) National Information Assurance Partnership

Management Response

SUBJECT: DoD OIG Draft Report for Management Advisory: The National Information Assurance Partnership's Evaluation and Certification Process for Commercial Off-the-Shelf Products (Project No. D2024-D000CU-0099.001)

DATE: 8/13/2025

FROM: Cybersecurity Directorate, NSA

AGREE with recommendation 1.a.1.

No later than 30 September 2025, NIAP will implement a procedure to conduct a search of public records for vulnerabilities disclosed after the Common Criteria Testing Laboratory's last vulnerability search, and resolve any found vulnerabilities with the Common Criteria Testing Laboratory before posting products on the Product Compliant List.

AGREE with recommendation 1.a.2

Effective immediately NIAP will conduct a review of statutes, executive orders, and other directives applicable to NSS owners, including National Security Agency directives, to determine whether the product has been prohibited from use before certifying a product for inclusion on the Product Compliant List.

AGREE with recommendation 1.b

NIAP will revise the Product Compliant List website to provide system owners clearer user interface to include core features for each product, full name of the protection profile, list of features tested and certified, and list of features not tested and not certified for use on National Security Systems by February 2026.

AGREE agrees with recommendation 1.c

NIAP has removed Ivanti Policy Secure and Ivanti Connect Secure from the Product Compliant List.

AGREE with recommendation 1.d.1

On 29 July 2025, NIAP Policy Letter #26 was published to clarify the applicability and relationship of U.S. laws, regulations, and directives to product acceptance into NIAP and inclusion of the NIAP PCL, as well as the withdrawal of a product previously certified by NIAP. This policy allows for the removal of a product that is prohibited from use on NSS by statue, executive order, or other directives applicable to NSS owners or operators, or the U.S. federal government.

(U) National Information Assurance Partnership (cont'd)

AGREE with recommendation 1.d.2

No later than 31 August 2025, NIAP will implement a procedure to post announcements to the webpage indicating a product removal and referencing the appropriate national directive.

(U) Right click on the X and select "Sign" to add a PKI digital signature:

X 

Gregory L. Smithberger
Acting Director
Cybersecurity Directorate
National Security Agency

(U) Acronyms and Abbreviations

(U) CCEVS	Common Criteria Evaluation and Validation Scheme
(U) CCTL	Common Criteria Testing Laboratories
(U) CNSSP	Committee on National Security Systems Policy
(U) COTS	Commercial Off-the-Shelf
(U) CVE	Common Vulnerabilities and Exposures
(U) ED	Emergency Directive
(U) ICS	Ivanti Connect Secure
(U) IPS	Ivanti Policy Secure
(U) IT	Information Technology
(U) NIAP	National Information Assurance Partnership
(U) NSA	National Security Agency
(U) NSS	National Security Systems
(U) PCL	Product Compliant List
(U) VPN	Virtual Private Network


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 www.dodig.mil/Components/Administrative-Investigations/Whistleblower-Reprisal-Investigations/Whistleblower-Reprisal/ or contact the Whistleblower Protection Coordinator at Whistleblowerprotectioncoordinator@dodig.mil

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

Legislative Affairs Division
703.604.8324

Public Affairs Division
public.affairs@dodig.mil; 703.604.8324

www.dodig.mil

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