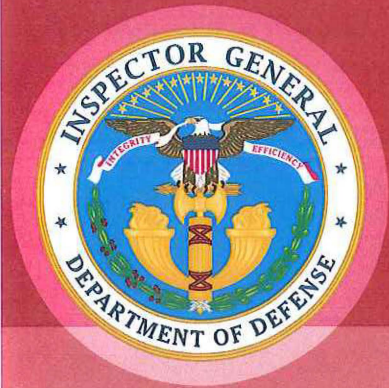


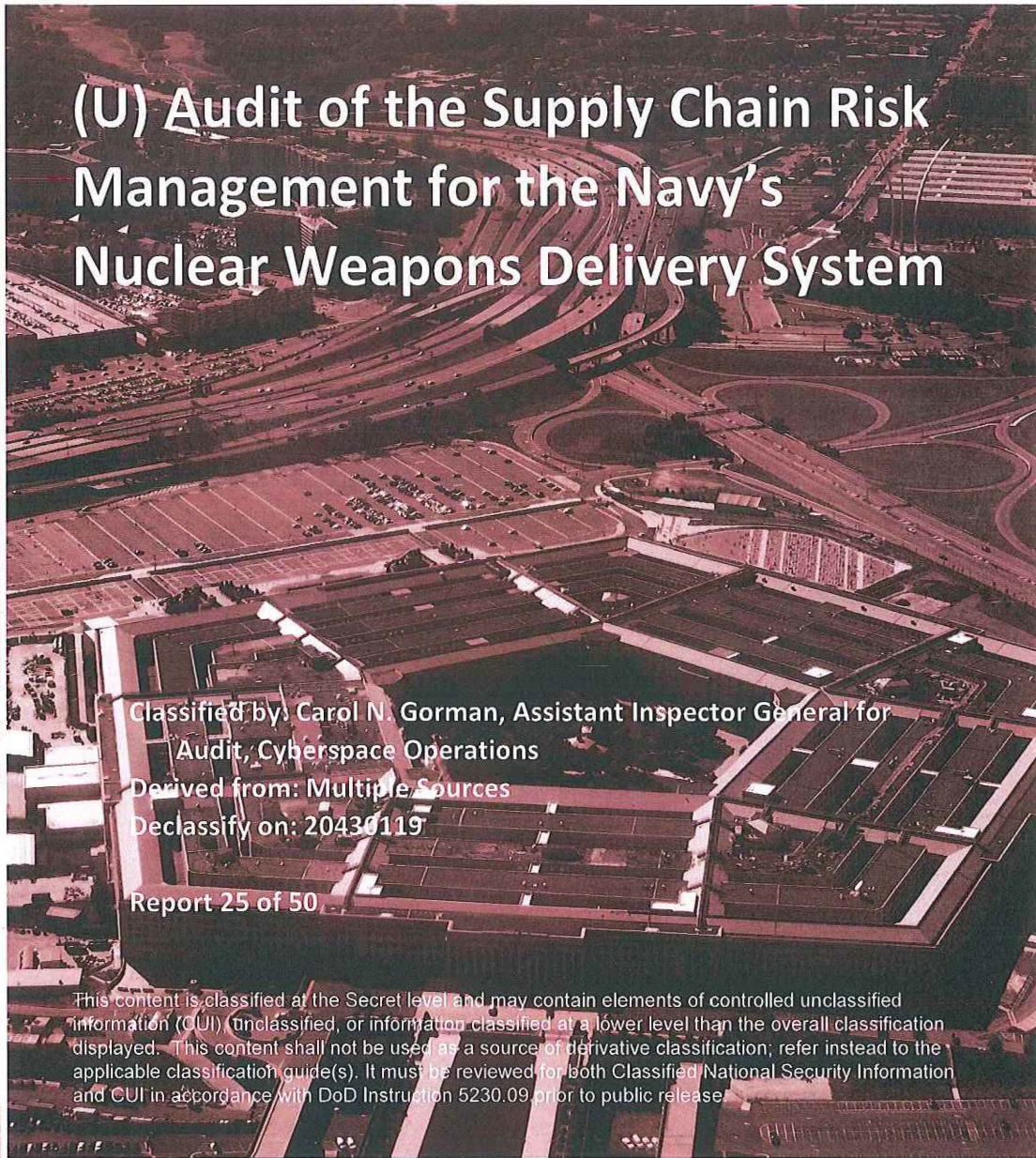
~~SECRET~~



# INSPECTOR GENERAL

*U.S. Department of Defense*

SEPTEMBER 1, 2020



## (U) Audit of the Supply Chain Risk Management for the Navy's Nuclear Weapons Delivery System

Classified by: Carol N. Gorman, Assistant Inspector General for Audit, Cyberspace Operations  
Derived from: Multiple Sources  
Declassify on: 20430119

Report 25 of 50

This content is classified at the Secret level and may contain elements of controlled unclassified information (CUI), unclassified, or information classified at a lower level than the overall classification displayed. This content shall not be used as a source of derivative classification; refer instead to the applicable classification guide(s). It must be reviewed for both Classified National Security Information and CUI in accordance with DoD Instruction 5230.09 prior to public release.

INTEGRITY ★ INDEPENDENCE ★ EXCELLENCE

Released by the DoD OIG FOIA Office  
under FOIA request DODOIG-2020-001182  
on \_\_\_\_\_

~~SECRET~~





# (U) Results in Brief

## (U) Audit of the Supply Chain Risk Management for the Navy's Nuclear Weapons Delivery System

(U) September 1, 2020

### (U) Objective

(U) The objective of this audit was to determine whether the Navy implemented supply chain risk management (SCRM) for the sea-based Trident II Strategic Weapons System (SWS) in accordance with DoD requirements.

(U) This is the fourth and final report in a series of audits conducted in response to a reporting requirement contained in House Report 114-537, to accompany the National Defense Authorization Act for Fiscal Year 2017. This audit focused on a U.S. nuclear weapons delivery system.

### (U) Background

(U) The DoD supply chain is the sequence of activities necessary to provide an end user with a finished product or system. Supply chain risk is the risk that an adversary may sabotage, maliciously introduce an unwanted function, or otherwise compromise the design, integrity, manufacturing, distribution, installation, operation, or maintenance of a system. SCRM is a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to reduce those threats.

(U) The Trident II SWS, a legacy sustainment system, is deployed aboard the *Ohio*-class Ship, Submersible, Ballistic, Nuclear Trident Submarines and comprises two systems, the Shipboard system and the Flight system. The Flight system is the nuclear portion of the delivery system, and consists of the Reentry, Missile, and Guidance subsystems.

### (U) Finding

(~~EU~~) Navy (b)(1) 1.7(e)  
[Redacted]

- (~~EU~~) Navy (b)(1) 1.7(e)  
[Redacted]
- (U) Navy (b)(1) 1.7(e)  
[Redacted]
- (S) Navy (b)(1) 1.4(a)(f)(g)(h)  
[Redacted]
- (~~EU~~) Navy (b)(1) 1.7(e)  
[Redacted]

(~~EU~~) Navy (b)(1) 1.7(e)  
[Redacted]

In addition, the Deputy Assistant Secretary of the Navy for Sustainment and the Deputy Assistant Secretary of the Navy for Research, Development, Test and Evaluation  
[Redacted]

Furthermore, Navy (b)(1) 1.7(e)  
[Redacted]

(S) Navy (b)(1) 1.4(a)(f)(g)(h), (b)(3)  
[Redacted]

<sup>1</sup> (U) A program protection plan is a tool to manage risk that supply chains will be exploited to destroy, modify, or exfiltrate critical data; degrade system performance; or decrease confidence in a system by helping programs adequately protect their technology, components,

(U) and information. Quality control processes are designed to ensure compliance with Navy specifications.



# (U) Results in Brief

## (U) Audit of the Supply Chain Risk Management for the Navy's Nuclear Weapons Delivery System

### (U) Finding (cont'd)

(S) Navy (b)(1) 1.4(a)(f)(g)(h), (b)(3) [redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]

### (U) Recommendations

(U) We recommend that the Under Secretary of Defense for Research and Engineering, in coordination with the Under Secretary of Defense for Acquisition and Sustainment and the DoD Chief Information Officer, revise DoD policy or issue clarifying guidance on implementing DoD SCRM requirements for legacy sustainment systems.

(CU) Navy (b)(1) 1.7(e), (b)(3) [redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]

(CU) In addition, we recommend that the Navy Strategic Systems Programs Director:

- (CU) Navy (b)(1) 1.7(e), (b)(3) [redacted]  
[redacted];
- (CU) Navy (b)(1) 1.7(e) [redacted]  
[redacted]  
[redacted];

### (U) Recommendations (cont'd)

- (S) Navy (b)(1) 1.4(a)(f)(g)(h) [redacted]  
[redacted]; and
- (CU) Navy (b)(1) 1.7(e) [redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted].

### (U) Management Comments and Our Response

(U) The Acting Director of Defense Research and Engineering for Research and Technology, responding for the Under Secretary of Defense for Research and Engineering, agreed to update DoD Instruction 5000.02T to clarify responsibilities for legacy system SCRM requirements. Therefore, the recommendation is resolved but will remain open.

(U) In oral comments, the Deputy Assistant Secretary of the Navy for Sustainment, responding for the Assistant Secretary of the Navy for Research, Development, and Acquisition, agreed Navy (b)(3) [redacted]  
[redacted] Therefore, the recommendation is resolved but will remain open.

(CU) The Director for the Navy Strategic Systems Programs Navy (b)(1) 1.7(e), (b)(3) [redacted]  
[redacted] Therefore, these recommendation are resolved but will remain open.



~~SECRET~~

# (U) Results in Brief

*(U) Audit of the Supply Chain Risk Management for the Navy's Nuclear Weapons Delivery System*

## *(U) Comments (cont'd)*

~~(U)~~ Navy (b)(1) 1.7(e), (b)(3)  
[Redacted text block consisting of six horizontal black bars]

Therefore, these recommendations are unresolved.

~~(U)~~ We request that the Director for Navy Strategic Systems Programs provide comments on the final report that describe actions that will be taken to implement the recommendations.

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

~~SECRET~~

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

<b>(U)</b> Management	Recommendations Unresolved	Recommendations Resolved	Recommendations Closed
Under Secretary of Defense for Research and Engineering		1	
Assistant Secretary of the Navy for Research, Development, and Acquisition		2	
Director, Navy Strategic Systems Programs	3.c, 3.d	3.a, 3.b	(U)

(U) Please provide Management Comments by October 1, 2020.

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

~~SECRET~~



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

September 1, 2020

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR RESEARCH AND  
ENGINEERING  
UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND  
SUSTAINMENT  
DOD CHIEF INFORMATION OFFICER  
ASSISTANT SECRETARY OF THE NAVY FOR RESEARCH,  
DEVELOPMENT AND ACQUISITION  
DIRECTOR FOR NAVY STRATEGIC SYSTEMS PROGRAMS  
AUDITOR GENERAL, DEPARTMENT OF THE NAVY

SUBJECT: Audit of the Supply Chain Risk Management for the Navy's Nuclear  
Weapons Delivery System  
(Report No. DODIG-2020-122)

(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 considered management's comments on the draft report when preparing the final report. These comments are included in the report.

(U) This report contains two recommendations that we consider unresolved because management officials did not agree or did not fully address the recommendations presented in the report. Therefore, as discussed in the Recommendations, Management Comments, and Our Response section of this report, these recommendations will remain open. We will track these recommendations until an agreement is reached on the actions that you will take to address the recommendations, and you have submitted adequate documentation showing that all agreed-upon actions are completed. Once we verify that the actions are complete, we will close the recommendations.

(U) This report contains four recommendations that we considered resolved and open. As discussed in the Recommendations, Management Comments, and Our Response sections of this report, we will close these recommendations when you provide us adequate documentation showing that all agreed-upon actions to implement the recommendations are completed.

~~SECRET~~

(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. For the resolved recommendations, please provide us within 90 days your response concerning specific actions in progress or completed on the recommendations. Send all responses to either **DoD OIG (b)(6)** if unclassified or **DoD OIG (b)(6)** and **DoD OIG (b)(6)** 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. Please direct questions to me at **DoD OIG (b)(6)**, (DSN **DoD OIG (b)(6)**).



Carol N. Gorman  
Assistant Inspector General for Audit  
Cyberspace Operations



## (U) Contents

<b>(U) Introduction .....</b>	<b>1</b>
(U) Objective.....	1
(U) Background .....	1
(U) Review of Internal Controls.....	6
<b>(U) Finding .....</b>	<b>8</b>
<del>(S)</del> Navy (b)(3) .....	8
(U) Navy (b)(1) 1.7(e) .....	9
<del>(S)</del> Navy (b)(1) 1.7(e) .....	16
<del>(S)</del> Navy (b)(3) .....	20
(U) Management Comments on the Finding and Our Response.....	20
(U) Recommendations, Management Comments, and Our Response .....	21
(U) Management Comments on the Response to the House Armed Services Committee Request and Our Response .....	29
<b>(U) Appendix A.....</b>	<b>31</b>
(U) Scope and Methodology .....	31
(U) Use of Computer-Processed Data.....	32
(U) Prior Coverage .....	32
<b>(U) Appendix B.....</b>	<b>35</b>
(U) House Armed Services Committee Request and Our Response.....	35
<b>(U) Appendix C.....</b>	<b>38</b>
<b>(U) Management Comments.....</b>	<b>39</b>
(U) Under Secretary of Defense for Research and Engineering.....	39
(U) Director, Navy Strategic Systems Programs.....	40
<b>(U) Sources of Classified Information .....</b>	<b>45</b>
<b>(U) Acronyms and Abbreviations.....</b>	<b>46</b>
<b>(U) Glossary .....</b>	<b>47</b>

## (U) Introduction

---

### (U) Objective

(U) The objective of this audit was to determine whether the Navy implemented supply chain risk management (SCRM) for a U.S. nuclear weapons delivery system in accordance with DoD requirements. We selected the sea-based Trident II Strategic Weapons System (SWS).

(U) We conducted this audit in response to a reporting requirement contained in House Report 114-537, to accompany the National Defense Authorization Act for FY 2017. This is the fourth and final report in a series of audits on DoD strategic capabilities SCRM. See Appendix A for scope, methodology, and prior audit coverage. See the Glossary for specialized terms used throughout the report.

### (U) Background

(U) The DoD supply chain is the sequence of activities necessary to provide an end user with a finished product or system (from raw material to finished product). Supply chain risk is the risk that an adversary may sabotage, maliciously introduce an unwanted function, or otherwise compromise the design, integrity, manufacturing, distribution, installation, operation, or maintenance of a system. The adversary may take actions to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of the system. SCRM is a systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to reduce those threats, whether presented by the supplier, the supplied product and its subcomponents, or the supply chain.

### ***(U) DoD OIG Legislative Reporting Requirement***

(U) In May 2016, the House Armed Services Committee expressed concerns that the DoD possessed limited data about the supply chain associated with certain critical systems.<sup>2</sup> The committee was also concerned that the DoD largely relies on assurances it receives from prime contractors, but those prime contractors often rely on subcontractors and others for information concerning the supply chain. The committee based its concerns on findings in a Government Accountability Office (GAO) audit report, which found that the DoD limited the Government-Industry Data Exchange Program's effectiveness because the DoD did not conduct oversight to ensure that

---

<sup>2</sup> (U) The committee expressed these concerns in House Report 114-537, to accompany H.R. 4907, the National Defense Authorization Act for Fiscal Year 2017.

(U) Defense agencies were reporting suspect counterfeit parts as required and DoD agencies limited industry's awareness of potential counterfeit issues.<sup>3</sup>

(U) The committee directed the DoD Office of Inspector General (DoD OIG) through House Report 114-537 to conduct an audit to evaluate and report on the supply chain security and assurance of the networks or systems deemed critical in the Missile Defense Agency, the Air Force Space Command, the Nuclear Command and Control System, and the delivery system or platform for U.S. nuclear weapons.<sup>4</sup> This report addresses the requirement to audit or evaluate a U.S. nuclear weapons delivery system. See Appendix B for the complete legislative requirement and the DoD OIG's responses.

### ***(U) Trident II Strategic Weapons System***

(U) The Trident II SWS, a legacy sustainment system, has been integral to the United States' nuclear deterrent strategy since 1990.<sup>5</sup> The Trident II SWS is deployed aboard the *Ohio*-class Ship, Submersible, Ballistic, Nuclear (SSBN) Trident submarines. The Navy's ballistic missile submarines provide an undetectable launch platform for the Trident II D5 sea-launched ballistic missiles and are designed specifically for stealth and the precision delivery of nuclear warheads. This delivery system was designed to be the most survivable leg of the nuclear triad and provide assured second-strike capability.<sup>6</sup>

(U) The Navy's 14 *Ohio*-class SSBNs typically operate for 15 or more years between major overhauls and have the capability to carry up to 24 Trident II D5 missiles with multiple independently targeted warheads.<sup>7</sup> Figure 1 shows the successful launch of a Trident II D5 missile from an *Ohio*-class SSBN.

---

<sup>3</sup> (U) Report No. GAO-16-236, "DoD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk," February 2016.

<sup>4</sup> (U) Based on an agreement made with subcommittee staffers, the DoD OIG has conducted a series of audits related to SCRM, and this audit is the fourth in the series. See Appendix A.

<sup>5</sup> (U) Navy (b)(1) 1.7(e)

<sup>6</sup> (U) The United States has maintained a nuclear triad consisting of manned bombers, land-based intercontinental ballistic missiles, and ballistic missile submarines capable of delivering nuclear weapons. Second-strike capability is the ability to launch a successful nuclear attack in response to a first strike attack on the United States.

<sup>7</sup> (U) The Strategic Arms Reduction Treaty of 1991 established limits on the *Ohio*-class SSBN and the Trident II D5 by deactivating four missile tubes.

(U) *Figure 1. Successful Trident II D5 Missile Launch*



(U) Source: Navy Submarine Force Pacific.

(U) The Trident II SWS consists of two systems, the Shipboard system and the Flight system. The Trident II SWS's Shipboard system consists of the Instrumentation, Navigation, Fire Control, and Launcher subsystems, which are located on each of the *Ohio*-class SSBNs. The Flight system, which is the nuclear portion of the delivery system, consists of the Reentry, Missile, and Guidance subsystems. These subsystems are contained in each one of the Trident II D5 Sea-Launched Ballistic Missiles, which are then loaded onto the SSBNs. The Trident II D5 Missile was designed to have a service life of 25 years when it was deployed on the *Ohio*-class SSBNs in 1990. However, according to the Assistant Secretary of the Navy for Research, Development, and Acquisition, the Trident II D5 Missile will be the initial payload for the *Ohio*-class SSBN replacement, the *Columbia*-class SSBN in 2031, and will serve throughout the remaining service life of the *Ohio*-class SSBN, which ends in 2040, about 25 years past the original service life.

### **(U) Trident II SWS Management and Support**

(U) The Offices of the Under Secretary of Defense for Research and Engineering, the Under Secretary of Defense for Acquisition and Sustainment, and the DoD Chief Information Officer are responsible for issuing policy for DoD SCRM requirements. The Deputy Assistant Secretary of the Navy for Sustainment (DASN[S]) and the Deputy Assistant Secretary of the Navy for Research, Development, Test, and Evaluation (DASN[RDT&E]) are the designated focal points for implementing and providing

(U) oversight of DoD SCRM policy for the Navy.<sup>8</sup> The Director for the Navy Strategic Systems Programs (SSP) and Defense Contract Management Agency (DCMA) officials are responsible for Trident II SWS management and support.

*(U) Strategic Systems Programs*

(U) The Navy SSP Director is responsible for all aspects of the research, development, production, logistics, storage, repair, and operational support of the Navy's Fleet Ballistic Missile Weapon Systems, including the Trident II SWS. The Director oversees the following offices to execute SCRM for the Trident II SWS.

- (U) Program Management Office:
  - ~~(U)~~ Navy (b)(3) [REDACTED]
  - ~~(U)~~ Navy (b)(3) [REDACTED]
  - ~~(U)~~ Navy (b)(3) [REDACTED]
  - ~~(U)~~ Navy (b)(3) [REDACTED]
- (U) Strategic Weapons Facility:
  - (U) provides Government inspection oversight and final acceptance inspection functions to verify contractual and design compliance; and
  - (U) monitors or witnesses the prime contractor's maintenance, operation, testing, receipt and inspection, and shipping of the Missile and Guidance subsystems.
- (U) Branch officials for the Missile subsystem (SP27) and Guidance subsystem (SP23):
  - (U) plan and execute the acquisition, life cycle support, and disposal of the Trident II SWS D5 Missile and Guidance subsystems;
  - (U) manage the research, design, development, and, testing for Guidance and Missile subsystems; and

<sup>8</sup> (U) Assistant Secretary of the Navy for Research, Development, and Acquisition Memorandum, "Realignment of the Assistant Secretary of the Navy for Research, Development, and Acquisition," September 27, 2019, stood up the DASN(S) and reassigned supply chain management from the DASN(RDT&E) to the DASN(S) effective October 1, 2019. The Office of the DASN(RDT&E) maintained its program protection responsibilities. Navy (b)(1) 1.7(e) [REDACTED]

- (U) establish, implement, and maintain quality control and monitoring systems.

### *(U) Defense Contract Management Agency*

(U) The DCMA provides contract administration services for the DoD, other Federal organizations, and international partners, and is an essential part of the acquisition process from pre-award to sustainment. The DCMA has a memorandum of agreement with the SSP Flight System Program Management Office to establish the DCMA's responsibilities for program support, engineering support, and contract administration for the Trident II SWS's Flight system subsystems.

### **(U) DoD Supply Chain Risk Management Policy**

(U) In 2009, the DoD reported to Congress that it developed a strategy to enable programs and system managers to conduct SCRM throughout a system life cycle.<sup>9</sup> Life cycle refers to all phases of the system's life, including research, development, test and evaluation, production, deployment, operations and support, and disposal. This strategy, referred to as the Strategy for Systems Assurance and Trustworthiness, stated that a partnership approach is critical for ensuring that supply chain risk is properly mitigated across mission-critical systems and networks. The report directed the Offices of the Under Secretary of Defense for Research and Engineering, the Under Secretary of Defense for Acquisition and Sustainment, and the DoD Chief Information Officer to jointly lead the effort to ensure that supply chain vulnerabilities in mission-critical systems are mitigated.<sup>10</sup>

(U) DoD Instruction 5200.44 establishes DoD SCRM policy for information and communications technology within national security systems to minimize the risk that the DoD's warfighting capability will be impaired because of vulnerabilities in system design or sabotage of a system's mission-critical functions or components by foreign intelligence, terrorists, or other adversaries.<sup>11</sup> The Instruction requires the application of risk management practices during the design phase and before purchasing or integrating critical components into their systems. Specifically, the Instruction requires program managers to conduct a criticality analysis to identify mission-critical functions and

---

<sup>9</sup> (U) "Report on Trusted Defense Systems in Response to National Defense Authorization Act, Section 254," December 22, 2009.

<sup>10</sup> (U) In 2018, the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics was reorganized into the Office of the Under Secretary of Defense for Acquisition and Sustainment and the Office of the Under Secretary of Defense for Research and Engineering. The responsibilities of the Office of the Assistant Secretary of Defense for Networks and Information Integration was assumed by the DoD Chief Information Officer in 2012.

<sup>11</sup> (U) DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012 (Incorporating Change 3, October 15, 2018).

(U) components and identify and manage risks and vulnerabilities associated with those critical components.

(U) An example of a risk mitigation technique is the use of threat assessments. Program managers are required to request intelligence threat assessments for suppliers of level I and level II critical components. Level I is assigned to a critical component that if compromised, would lead to total mission failure. Level II is assigned to a critical component, that if compromised, would significantly impact the mission or involves unacceptable degradation.<sup>12</sup> The results from the assessment should then be used to develop risk mitigation activities. DoD Instruction 5200.44 requires program managers to document the results of the criticality analysis and risk management activities in a program protection plan (PPP). A PPP guides a program manager's efforts and the actions of others to manage the risk to critical program information and mission-critical functions and components associated with the program.

(U) A July 18, 2011, memorandum from the Principal Deputy Under Secretary of Defense for Acquisition, Technology, and Logistics (now the Principal Deputy Under Secretary of Defense for Acquisition and Sustainment) directs program managers to use the PPP Outline and Guidance developed by the Deputy Assistant Secretary of Defense for Systems Engineering.<sup>13</sup> The PPP Outline and Guidance defines the minimum requirements for program protection that comply with DoD policy and provides program offices with guidance regarding the content, organization, and development of PPPs. Furthermore, the PPP Outline and Guidance and DoD Instruction 5000.02T state that organizations should update the PPP throughout the acquisition life cycle as threats and vulnerabilities change or are better understood and after any contract award.<sup>14</sup> In addition, the Defense Acquisition Guidebook provides program offices with best practices for performing risk analyses, evaluating vulnerabilities, identifying threats, and developing mitigation activities.

## (U) Review of Internal Controls

~~(U)~~ DoD Instruction 5010.40 requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls.<sup>15</sup>

---

<sup>12</sup> (U) The level III and level IV criticality designations are not prioritized for threat assessments because of their acceptable or negligible impact on mission success.

<sup>13</sup> (U) Principal Deputy Under Secretary of Defense for Acquisition, Technology, and Logistics Memorandum, "Document Streamlining – Program Protection Plan (PPP)," July 18, 2011; and Deputy Assistant Secretary of Defense for Systems Engineering, "Program Protection Plan Outline and Guidance," July 2011.

<sup>14</sup> (U) DoD Instruction 5000.02T, "Operation of the Defense Acquisition System," January 7, 2015 (Incorporating Change 7, April 23, 2020).

<sup>15</sup> (U) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

~~(U)~~ We identified Navy (b)(3) [REDACTED] in the DoD SCRM program. Specifically, Navy (b)(3) [REDACTED]

[REDACTED]  
[REDACTED] In addition, Navy (b)(3) [REDACTED]

[REDACTED] We will provide a copy of the report to the senior official responsible for internal controls in the Offices of the Under Secretary of Defense for Acquisition and Sustainment; the Under Secretary of Defense for Research and Engineering; the DoD Chief Information Officer; the Assistant Secretary of the Navy for Research, Development, and Acquisition; and Navy SSP.



## (U) Finding

~~(CUI)~~ Navy (b)(1) 1.7(e)

[Redacted]

~~(CUI)~~ Navy (b)(1) 1.7(e)

[Redacted]

- ~~(CUI)~~ Navy (b)(1) 1.7(e)  
[Redacted]
- (U) Navy (b)(1) 1.7(e)  
[Redacted]
- ~~(S)~~ Navy (b)(1) 1.4(a)(f)(g)(h)  
[Redacted]
- ~~(CUI)~~ Navy (b)(1) 1.7(e)  
[Redacted]

~~(CUI)~~ Navy (b)(1) 1.7(e)

[Redacted]

~~(S)~~ Navy (b)(1) 1.4(a)(f)(g)(h)

[Redacted]

<sup>16</sup> (U) A program protection plan is a tool to manage risk that supply chains will be exploited to destroy, modify, or exfiltrate critical data; degrade system performance; or decrease confidence in a system by helping programs adequately protect their technology, components, and information. Quality control processes are designed to ensure compliance with Navy specifications.

(U) Navy (b)(1) 1.7(e) [Redacted]

(S) Navy (b)(1) 1.4(a)(f)(g)(h) [Redacted]

(U) Navy (b)(3) [Redacted]

(CU) Navy (b)(1) 1.7(e) [Redacted]

(CU) Navy (b)(1) 1.7(e) [Redacted]

(U) Specifically, the Trident II SWS Navy (b)(1) 1.7(e)

- (CU) Navy (b)(3) [Redacted]

- ~~(U)~~ Navy (b)(3) [Redacted]
- ~~(U)~~ Navy (b)(3) [Redacted]

~~(U)~~ Navy (b)(3) [Redacted]

~~(U)~~ Navy (b)(1) 1.7(e), (b)(3) [Redacted]

~~(S)~~ Navy (b)(1) 1.4(a)(f)(g)(h) [Redacted]

~~(S)~~ Navy (b)(1) 1.4(a)(f)(g)(h) [Redacted]

~~(S)~~ Navy (b)(1) 1.4(a)(f)(g)(h) [Redacted]

(U) Navy (b)(3) [Redacted]

~~(S)~~ Navy (b)(1) 1.4(a)(f)(g)(h) [Redacted]

~~(CU)~~ Navy (b)(3) [Redacted]

~~(CU)~~ Navy (b)(3) [Redacted]

<sup>17</sup> (U) Secondary sources are subcontractors.

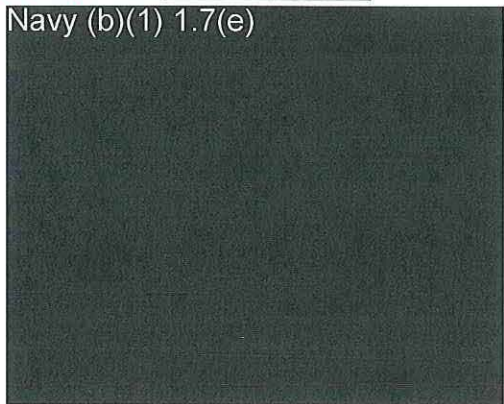
<sup>18</sup> ~~(CU)~~ Navy (b)(3) [Redacted]

(S) Navy (b)(1) 1.4(a)(f)(g)(h) [Redacted]

(U) The Missile subsystem:

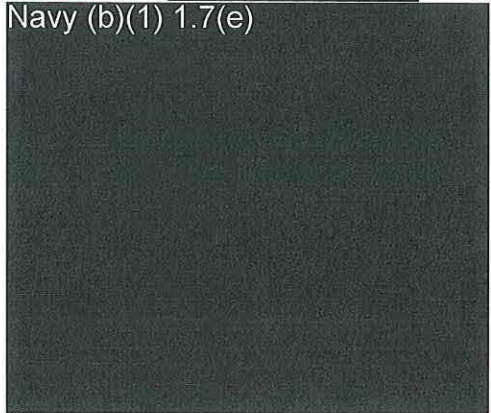
- (CU) Navy (b)(1) 1.7(e) [Redacted]
- (CU) Navy (b)(1) 1.7(e) [Redacted]
- (CU) Navy (b)(1) 1.7(e) [Redacted]
- (CU) Navy (b)(1) 1.7(e) [Redacted]

(U) Figure 2. Navy (b)(1) 1.7(e)



(U) Source: Navy SSP.

(U) Figure 3. Navy (b)(1) 1.7(e)

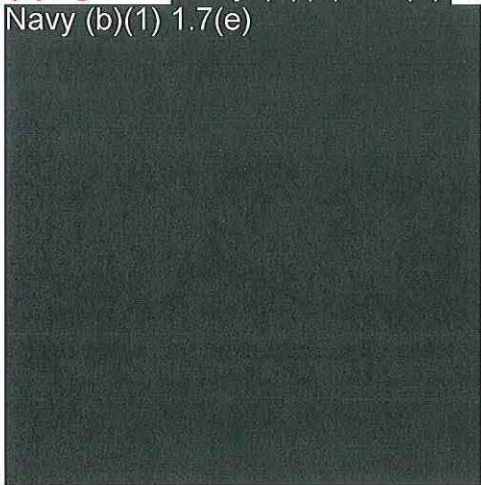


(U) Source: Navy SSP.

(U) The Guidance subsystem:

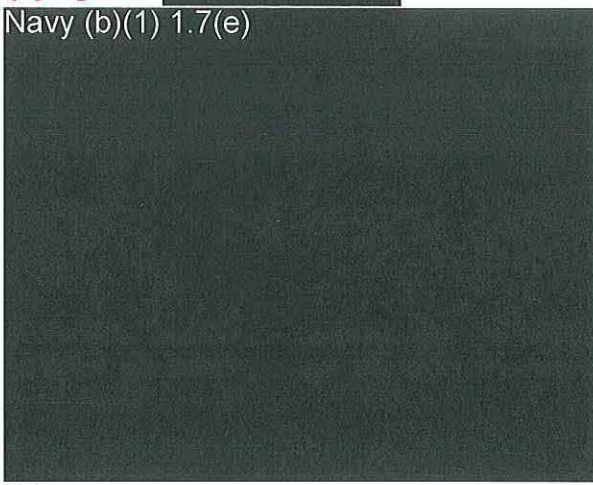
- ~~(S)~~ Navy (b)(1) 1.7(e) [Redacted]
- ~~(S)~~ Navy (b)(1) 1.7(e) [Redacted]

(U) Figure 4. Navy (b)(1) 1.7(e)



(U) Source: Navy SSP.

(U) Figure 5. Navy (b)(1) 1.7(e)



(U) Source: Navy SSP.

~~(S)~~ Navy (b)(1) 1.7(e) [Redacted]

(U) Navy (b)(3) [Redacted]

(U) Navy (b)(3) [Redacted]

(U) Navy (b)(3) [Redacted]

*(U) Quality of Missile Subsystem Subcomponents*

~~(U)~~ Navy (b)(1) 1.7(e) [Redacted]

- ~~(U)~~ Navy (b)(1) 1.7(e) [Redacted]
- ~~(U)~~ Navy (b)(1) 1.7(e) [Redacted]
- ~~(U)~~ Navy (b)(1) 1.7(e) [Redacted] <sup>21</sup>

<sup>19</sup> (U) Navy (b)(3) [Redacted]

<sup>20</sup> (U) Navy (b)(3) [Redacted]

<sup>21</sup> (U) Navy (b)(3) [Redacted]

~~(S)~~ Navy (b)(1) 1.7(e) [redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]

~~(S)~~ Navy (b)(1) 1.7(e) [redacted]  
[redacted]  
[redacted]  
[redacted]

- ~~(S)~~ Navy (b)(1) 1.7(e) [redacted]
- ~~(S)~~ Navy (b)(1) 1.7(e) [redacted]  
[redacted]
- ~~(S)~~ Navy (b)(1) 1.7(e) [redacted]  
[redacted]

~~(S)~~ Navy (b)(1) 1.7(e) [redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]  
[redacted]

~~(S)~~ Navy (b)(1) 1.7(e) [redacted]  
[redacted]  
[redacted]

<sup>22</sup> (U) Navy (b)(1) 1.7(e) [redacted]  
[redacted]

<sup>23</sup> (U) Navy (b)(1) 1.7(e) [redacted]  
[redacted]



~~(CU)~~ Navy (b)(1) 1.7(e) [Redacted]

~~(CU)~~ Navy (b)(1) 1.7(e) [Redacted]

~~(CU)~~ Navy (b)(1) 1.7(e) [Redacted]

**(U) DoD Did Not Establish Clear SCRM Guidance**

~~(CU)~~ Navy (b)(1) 1.7(e) [Redacted]

~~(CU)~~ DoD Instruction 5200.44 policy states, "The application of risk management practices shall begin during the design of applicable systems and before the acquisition of critical components or their integration within applicable systems, whether acquired through a commodity purchase, system acquisition, or sustainment process." The Instruction includes requirements for identifying and managing risk and for conducting a criticality analysis during the initial design of a program through sustainment. Risk management and a criticality analysis are key controls to help protect the DoD's critical systems. However, the Instruction does not include requirements for identifying and managing risk and for conducting a criticality analysis if the program was in sustainment prior to the issuance of the Instruction.

~~(S)~~ Navy (b)(1) 1.4(a)(f)(g)(h), (b)(3); OSD/JS (b)(1) 1.4(a)  
[Redacted]

~~(CU)~~ Navy (b)(1) 1.7(e)  
[Redacted]

~~(CU)~~ Navy (b)(1) 1.7(e)  
[Redacted]

~~(CU)~~ Navy (b)(1) 1.7(e)  
[Redacted]

~~(CU)~~ Navy (b)(1) 1.7(e)  
[Redacted]

(~~EU~~) Navy (b)(1) 1.7(e) [Redacted]

(~~EU~~) Navy (b)(1) 1.7(e) [Redacted]

(~~EU~~) Navy (b)(1) 1.7(e) [Redacted]

<sup>24</sup> (U) Navy (b)(1) 1.7(e) [Redacted]

<sup>25</sup> (U) Navy (b)(1) 1.7(e) [Redacted]

<sup>26</sup> (U) Navy (b)(1) 1.7(e) [Redacted]

<sup>27</sup> (U) Navy (b)(1) 1.7(e) [Redacted]

~~(CU)~~ Navy (b)(1) 1.7(e) [Redacted]  
[Redacted]

~~(CU)~~ Navy (b)(1) 1.7(e) [Redacted]  
[Redacted]  
[Redacted]  
[Redacted] [Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

~~(CU)~~ Navy (b)(1) 1.7(e) [Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

~~(CU)~~ Navy (b)(1) 1.7(e) [Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

<sup>28</sup> (U) Navy (b)(1) 1.7(e) [Redacted]  
[Redacted]

~~(CUI)~~ Navy (b)(1) 1.7(e) [Redacted]

~~(S)~~ Navy (b)(1) 1.4(a)(f)(g)(h) [Redacted]

### (U) Management Comments on the Finding and Our Response

*(U) Director for the Navy Strategic Systems Programs Director Comments*

~~(CUI)~~ Navy (b)(1) 1.7(e) [Redacted]

<sup>29</sup> (U) The National Defense Strategy, "Sharpening the American Military's Competitive Edge," January 19, 2018.

*(U) Our Response*

~~(U)~~ Navy (b)(1) 1.7(e)  
[Redacted text block]

~~(S)~~ Navy (b)(1) 1.4(a)(f)(g)(h)  
[Redacted text block]

~~(U)~~ Navy (b)(1) 1.7(e)  
[Redacted text block]

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

***(U) Recommendation 1***

**(U) We recommend that the Under Secretary of Defense for Research and Engineering, in coordination with the Under Secretary of Defense for Acquisition and Sustainment and the DoD Chief Information Officer, revise DoD Instruction 5200.44 or issue clarifying guidance to implement DoD supply chain risk management requirements for legacy sustainment systems.**

*(U) Under Secretary of Defense for Research and Engineering Comments*

(U) The Acting Director of Defense Research and Engineering for Research and Technology, responding for the Under Secretary of Defense for Research and Engineering, agreed, stating that the Under Secretary for Research and Engineering, the Under Secretary of Defense for Acquisition and Sustainment, and the DoD Chief Information Officer were updating DoD Instruction 5000.02T to clarify SCRM responsibilities for legacy systems under the Adaptive Acquisition Reform initiative led by Under Secretary of Defense for Acquisition and Sustainment. The Acting Director stated that updates to DoD Instruction 5000.02T were expected by December 31, 2020.

*(U) Our Response*

(U) Comments from the Acting Director addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once we verify that DoD Instruction 5000.02T includes SCRM requirements and responsibilities for legacy sustainment systems.

**(U) Recommendation 2**

~~(S)~~ Navy (b)(1) 1.7(e), (b)(3)

[REDACTED]

*(U) Assistant Secretary of the Navy for Research, Development, and Acquisition Comments*

(U) In oral comments, the DASN(S), responding for the Assistant Secretary of the Navy for Research, Development, and Acquisition, agreed, Navy (b)(3)

[REDACTED]

*(U) Our Response*

(U) Comments from the DASN(S) addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once we verify that Navy (b)(3)

(U) Navy (b)(3) [Redacted]

**(U) Recommendation 3**

(U) We recommend that the Director for the Navy Strategic Systems Programs:

- a. ~~(U)~~ Navy (b)(1) 1.7(e), (b)(3) [Redacted]

*(U) Director for the Navy Strategic Systems Programs Comments*

~~(U)~~ Navy (b)(1) 1.7(e) [Redacted]

*(U) Our Response*

~~(U)~~ Comments from the Director addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. Navy (b)(1) 1.7(e) [Redacted]

- b. ~~(U)~~ Navy (b)(1) 1.7(e) [Redacted]

*(U) Director for the Navy Strategic Systems Programs Comments*

~~(U)~~ Navy (b)(1) 1.7(e) [Redacted]



*(U) Our Response*

~~(CU)~~ Comments from the Director addressed all specifics of the recommendation; therefore, the recommendation is resolved but will remain open. We will close the recommendation once we verify that the Navy SSP ~~Navy (b)(1) 1.7(e), (b)(3)~~

c. ~~(S)~~ ~~Navy (b)(1) 1.4(a)(f)(g)(h), (b)(3); OSD/JS (b)(1) 1.4(a)~~

*(U) Director for the Navy Strategic Systems Programs Comments*

~~(CU)~~ ~~Navy (b)(1) 1.7(e), (b)(3)~~

*(U) Our Response*

~~(S)~~ Comments from the Director did not address the specifics of this recommendation; therefore, the recommendation is unresolved. ~~Navy (b)(1) 1.4(a)(f)(g)(h), (b)(3)~~

*(U) Under Secretary of Defense for Research and Engineering  
Unsolicited Comments*

~~(S)~~ Navy (b)(1) 1.4(a)(f)(g)(h), (b)(3), (b)(5); OSD/JS (b)(1) 1.4(a)  
[Redacted]

*(U) Our Response*

~~(S)~~ Navy (b)(1) 1.4(a)(f)(g)(h)  
[Redacted]

d. ~~(CU)~~ Navy (b)(1) 1.7(e)  
[Redacted]

*(U) Director for the Navy Strategic Systems Programs Comments*

~~(CU)~~ Navy (b)(3)  
[Redacted]

~~(CU)~~ Navy (b)(1) 1.7(e)  
[Redacted]

~~(CU)~~ Navy (b)(1) 1.7(e) [Redacted]

~~(CU)~~ Navy (b)(1) 1.7(e) [Redacted]

~~(CU)~~ Navy (b)(1) 1.7(e) [Redacted]

*(U) Our Response*

~~(CU)~~ Comments from the Director did not address this recommendation; therefore, the recommendation is unresolved. Navy (b)(1) 1.7(e) [Redacted]

(~~CU~~) Navy (b)(1) 1.7(e) [Redacted]

(~~CU~~) Navy (b)(1) 1.7(e) [Redacted]

(~~CU~~) Navy (b)(1) 1.7(e) [Redacted]

(~~CU~~) Navy (b)(1) 1.7(e)  
[Redacted text block]

(~~CU~~) Navy (b)(1) 1.7(e)  
[Redacted text block]

(~~S~~) Navy (b)(1) 1.4(a)(f)(g)(h)  
[Redacted text block]

~~(S)~~ Navy (b)(1) 1.4(a)(f)(g)(h)  
[Redacted]

(U) We request that the Director provide additional comments on the final report on how the Navy SSP will improve Government oversight and quality controls for the Trident II SWS.

### **(U) Management Comments on the Response to the House Armed Services Committee Request and Our Response**

*(U) Director for the Navy Strategic Systems Programs Comments*

~~(EU)~~ Navy (b)(1) 1.7(e)  
[Redacted]

~~(EU)~~ Navy (b)(1) 1.7(e)  
[Redacted]

*(U) Our Response*

~~(EU)~~ Navy (b)(1) 1.7(e)  
[Redacted]

~~(U)~~ Navy (b)(1) 1.7(e) [Redacted]

[Redacted]. Based on the Director's comments, we revised our response to Question 1 from the House Armed Service Committee to include additional details of actions taken by the Navy SSP.

~~(U)~~ Navy (b)(1) 1.7(e) [Redacted]

## (U) Appendix A

### (U) Scope and Methodology

(U) We conducted this performance audit from April 2019 through February 2020 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 interviewed officials from the Office of the Under Secretary of Defense for Acquisition and Sustainment, the Office of the Under Secretary of Defense for Research and Engineering, and the Department of the Navy SSP to discuss SCRM policy requirements and obtain background information on the Trident II SWS. We interviewed SSP and Program Management Office officials, prime contractors, and major subcontractors for the Trident II SWS to determine how they implemented SCRM requirements for the Missile and Guidance subsystems. In addition, we interviewed Navy and prime contractor officials at the Strategic Weapons Facilities that support the on-load and off-load of the subsystems on the *Ohio*-class SSBNs to determine quality assurance procedures in place for the Missile and Guidance subsystems. We also interviewed Naval Surface Warfare Center Crane Division officials responsible for providing engineering and component acceptance test services for the Trident II SWS.

(U) We reviewed the Trident II SWS PPP, dated April 25, 2017, to determine whether the PPP included minimum DoD requirements outlined in the PPP Outline and Guidance criteria and was updated after Trident II SWS contracts were awarded. We also reviewed Trident II SWS PPP to determine whether **Navy (b)(3)**

[REDACTED]

[REDACTED] We selected the Trident II SWS's Missile and Guidance subsystems for review to answer congressional questions and **Navy (b)(3)**

[REDACTED]

[REDACTED] We also reviewed the Navy's nuclear safety ordnance document, and interviewed Navy officials to **Navy (b)(3)** to the Missile and Guidance subsystems.<sup>30</sup>

<sup>30</sup> (U) **Navy (b)(3)**

[REDACTED]



(U) In addition, we reviewed 11 contracts ongoing at the time of the audit that Navy SSP awarded from July 2014 to February 2019 used to procure parts for the Missile and Guidance subsystems and to identify the prime contractors for the Trident II SWS, SCRM-related requirements, and Defense Federal Acquisition Regulation Supplement clauses. Specifically, we reviewed the following five contracts for the Missile subsystem.

- (U) N00030-14-C-0100
- (U) N00030-15-C-0100
- (U) N00030-16-C-0100
- (U) N00030-17-C-0100
- (U) N00030-18-C-0100

(U) Furthermore, we reviewed the following six contracts for the Guidance subsystem.

- (U) N00030-15-C-0003
- (U) N00030-16-C-0008
- (U) N00030-16-C-0014
- (U) N00030-17-C-0008
- (U) N00030-19-C-0001
- (U) N00030-19-C-0008

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

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

### **(U) Prior Coverage**

(U) During the last 5 years, the GAO and the DoD OIG issued four reports discussing SCRM. Unrestricted GAO reports can be accessed at <http://www.gao.gov>. Unrestricted DoD OIG reports can be accessed at <http://www.dodig.mil/reports.html/>.

### **(U) GAO**

(U) Report No. GAO-16-236, "Counterfeit Parts: DoD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk," February 16, 2016

(U) The GAO reviewed defense agencies' and contractors' reporting of counterfeit parts and the detection and avoidance of counterfeit parts in the DoD supply chain. The GAO identified that the DoD limited the Government-Industry Data Exchange

(U) Program's effectiveness because the DoD is not conducting oversight to ensure that Defense agencies are reporting suspect counterfeit parts as required; standardized processes did not exist for establishing when, based on extent of evidence, to report suspect counterfeit parts; and DoD agencies typically limited access of suspect counterfeit parts reports to Government agencies, thereby limiting industry's awareness of potential counterfeit issues.

(U) In addition, the GAO reported that the DoD has not finalized how the counterfeit parts detection and avoidance systems of contractors will be assessed. According to the GAO, until the DoD clarifies criteria for contractors on how their systems will be evaluated, it cannot fully ensure these systems detect and avoid electronic counterfeit parts.

**(U) DoD OIG**

(U) DODIG-2020-066, "Audit of the Department of Defense Supply Chain Risk Management Program for Nuclear Command, Control, and Communications Systems," March 2, 2020

~~(S)~~ Navy (b)(1) 1.4(a)(f)(g)(h)  
[Redacted text block]

(U) Report No. DODIG-2018-143, "Air Force Space Command Supply Chain Risk Management of Strategic Capabilities," August 14, 2018

~~(CUI)~~ The DoD OIG identified that the Air Force Space Command did not fully implement DoD SCRM policy because it did not establish the controls and oversight necessary to conduct a thorough criticality analysis to identify critical components and submit complete and accurate requests for threat assessments to the [Redacted] Navy (b)(1) 1.7(e) [Redacted]. In addition, the DoD OIG identified that the Air Force Space Command did not require the purchase of application-specific integrated circuits from suppliers approved by the Defense Microelectronics Activity and did not

~~(S)~~ ensure the use of test and evaluation capabilities Navy (b)(1) 1.7(e)  
[REDACTED].

(U) Report No. DODIG-2017-076, "The Missile Defense Agency Can Improve Supply Chain Security for the Ground-Based Midcourse Defense System," April 27, 2017

~~(S)~~ The DoD OIG identified that the Missile Defense Agency did not establish controls and oversight necessary to maintain an accurate critical components list to manage risks to the Ground-Based Midcourse Defense System throughout its life cycle and prioritize the list for supplier threat assessment requests to vet critical component suppliers for the system. In addition, the Missile Defense Agency did not identify the suppliers of all critical components or use rigorous test and evaluation capabilities to detect vulnerabilities within critical components.

## **(U) Appendix B**

### **(U) House Armed Services Committee Request and Our Response**

#### ***(U) House Armed Services Committee Request***

(U) The House Armed Services Committee expressed concerns related to supply chain security in House Report 114-537. Specifically, the committee stated that is aware of the report submitted by GAO, "DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk," (GAO-16-236) in February 2016. The committee noted the finding that, "DoD contractors rely on thousands of subcontractors and suppliers, including the original component manufacturers that assemble microcircuits and the mid-level manufacturers subcontracted to develop the individual subsystems that make up a complete system or supply."

(U) In addition, the committee expressed concerns that, as a practical matter, it appears that the Department possesses very little real data about the supply chain associated with certain critical systems. The committee also noted an appearance that the Department largely relies on assurances it receives from prime contractors, but oftentimes those prime contractors rely on subcontractors and others for information regarding supply chains and there may be little or no actual data on which to base their assurances to the Department.

(U) House Report 114-537 goes on to state that the committee is aware that the Department recently promulgated Defense Federal Acquisition Regulation Supplement Subpart 239.73 ("Requirements For Information Relating To Supply Chain Risk"), but the committee is concerned that there has been little practical progress in implementing these regulations. Moreover, even when implemented, an approach that relies primarily (or exclusively) on simply analyzing threat intelligence in Government databases will almost certainly not generate sufficient data about actual hardware and software components and subcomponents necessary to understand critical supply chains.

(U) The House Armed Services Committee identified specific matters that the DoD OIG should address as follows.

1. (U) Does the Defense agency or Military Service responsible for the particular system or network conduct actual forensic evaluations of the supply chain associated with the system or network? Does the agency or service rely on the representations of U.S. suppliers or does it perform independent verification

(U) and validation of the source of supply for each critical component and subcomponent of U.S. branded products or systems?

2. (U) For software, firmware, and chip design that is deemed by the command or agency to be critical to the reliability and performance of the designated network or system, can the service or agency (or its suppliers) identify by name and nationality the developers involved?
3. (U) How much diligence has been performed by the service or agency on second and third-tier suppliers?

**(U) Our Response**

1. ~~(S)~~ Navy (b)(1) 1.7(e) [Redacted]
2. (U) Navy (b)(3) [Redacted]
3. ~~(S)~~ Navy (b)(1) 1.4(a)(f)(g)(h) [Redacted]

(S) Navy (b)(1) 1.4(a)(f)(g)(h)  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]  
[Redacted]

## (U) Appendix C

~~(U)~~ Navy (b)(1) 1.7(e)

A large black rectangular redaction box covers the majority of the page's content, starting below the section header and extending nearly to the bottom of the page.

Navy (b)(1) 1.7(e)

## (U) Management Comments

### (U) Under Secretary of Defense for Research and Engineering



RESEARCH  
AND ENGINEERING

~~SECRET~~

OFFICE OF THE UNDER SECRETARY OF DEFENSE  
3030 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3030

MEMORANDUM FOR PROGRAM DIRECTOR FOR AUDIT CYBERSPACE OPERATIONS

SUBJECT: USD(R&E) Response to Draft Report for the "Audit of the Supply Chain Risk Management for the Navy's Nuclear Weapons Delivery System" (Project No. D2019-D000CT-013.00)

I have reviewed the draft report and appreciate the opportunity to provide comments on the recommendations to the DoD Inspector General (IG).

(U) IG Recommendation 1: Concur. Under Secretary of Defense for Research and Engineering, Under Secretary of Defense for Acquisition and Sustainment and Department of Defense Chief Information Officer have been coordinating on DoDI 5000.02 policy updates to clarify responsibilities for DoD Supply Chain Risk Management requirements for legacy systems under the Adaptive Acquisition Reform initiative led by USD(A&S). DoDI 5000.02 policy updates are planned to be completed by December 31, 2020.

IG Recommendation 3, bullet 3: Partially concur. Navy (b)(1) 1.4(a)(f)(g)(h), (b)(5) OSD/JS (b)(1) 1.4(a)

Please contact [redacted] if additional information is required.

LEI.JIH-  
FEN [redacted]

JihFen Lei  
Acting Director of Defense Research and  
Engineering for Research and Technology

Enclosure:  
As stated

~~SECRET~~



## (U) Director, Navy Strategic Systems Programs



~~CONTROLLED UNCLASSIFIED INFORMATION~~

DEPARTMENT OF THE NAVY  
DIRECTOR, STRATEGIC SYSTEMS PROGRAMS  
1250 10<sup>TH</sup> STREET SE, SUITE 3600  
WASHINGTON NAVY YARD, DC 20374-5127

7566  
Ser SP00G/071320001  
15 Jul 20

From: Director, Strategic Systems Programs  
To: Department of Defense Inspector General

Subj: (U) STRATEGIC SYSTEMS PROGRAMS RESPONSE TO AUDIT OF THE SUPPLY CHAIN RISK MANAGEMENT FOR THE NAVY'S NUCLEAR WEAPON DELIVERY SYSTEM

Ref: (a) Audit of the Supply Chain Risk Management for Navy's Nuclear Weapon Delivery System of 13 Mar 20, Project Number D2019-D000CT-0138.000

Encl: (1) SSP Response to the DOD IG Draft Report, "Audit of the Supply Chain Risk Management for Navy's Nuclear Weapon Delivery System" of 13 Mar 20, Project Number D2019-D000CT-0138.000

1. Strategic Systems Programs (SSP) has reviewed the findings and associated recommendations contained in reference (a), and the enclosed responses are provided for the record.
2. The Department of the Navy, Strategic Systems Programs (SSP) has reviewed the subject report and provides the following summary comments.

a. Nav (b)(1) 1.7(e)

[Redacted]

b. Nav (b)(1) 1.7(e)

[Redacted]

3. Details on the high-level comments in paragraph 2 are provided in enclosure (1). The point of contact for this matter is [Redacted]

Controlled by: SSP  
CUI Category: DEFENSE  
Distribution/Dissemination Controls: DL ONLY  
POC: Navy (b)(6)

J. R. WOLFE, JR

~~CONTROLLED UNCLASSIFIED INFORMATION~~

(U) Director, Navy Strategic Systems Programs (cont'd)

~~CONTROLLED UNCLASSIFIED INFORMATION~~

**SSP RESPONSE TO THE DOD IG DRAFT REPORT**  
**“Audit of the Supply Chain Risk Management for Navy’s Nuclear Weapon Delivery System” of 13 Mar 20, Project Number D2019-D000CT-0138.000**

1. For over 30 years, the TRIDENT II D5 Strategic Weapons System (SWS), along with its Life Extended (LE) alteration, has met all Combatant Commander and Fleet Commander weapons systems performance requirements in support of the Nation’s nuclear deterrent. As a result of its unprecedented performance and reliability, the TRIDENT II D5 SWS is able to provide nearly 70% of our Nation’s nuclear deterrent. Navy (b)(1) 1.7(e)

has been refined and demonstrated throughout the Navy (b)(1) 1.7(e)

The D5 SWS is a highly complex system Navy (b)(1) 1.7(e)

Navy (b)(1) 1.7(e)

we have taken every appropriate action to maintain compliance with every applicable law, regulation, and policy. It is our position that while agreeing with the intent of the recommendations provided in the report there were no deficiencies related to law, regulation, or policy compliance. Navy (b)(1) 1.7(e)

2. In light of the above considerations Navy (b)(1) 1.7(e) SSP offers the following responses to the recommendations made by the DoD IG.

a. Recommendation 3.a. Navy (b)(1) 1.7(e), (b)(3)

[Redacted]

Nevertheless,

SSP concurs with this recommendation in light of work already underway by SSP Navy (b)(1) 1.7(e)

b. Recommendation 3.b. Navy (b)(1) 1.7(e)

[Redacted]

Controlled by: DON  
Controlled by: SSP  
CUI Category: DEFENSE  
Distribution/Dissemination Controls: DL ONLY  
POC: Navy (b)(6)

Enclosure (1)

~~CONTROLLED UNCLASSIFIED INFORMATION~~

**(U) Director, Navy Strategic Systems Programs (cont'd)**

~~CONTROLLED UNCLASSIFIED INFORMATION~~

c. Recommendation 3.c. Navy (b)(1) 1.7(e); (b)(3)

[Redacted]

d. Recommendation 3.d. Navy (b)(1) 1.7(e), (b)(3)

[Redacted]

Navy (b)(1) 1.7(e)

[Redacted]

Navy (b)(1) 1.7(e)

[Redacted]

SSP has full confidence in the performance of its prime contractors and subcontractors, with whom it has decades' long relationships in the production of the Navy's sea-based strategic deterrent.

Navy (b)(1) 1.7(e)


[Redacted]

~~CONTROLLED UNCLASSIFIED INFORMATION~~

**(U) Director, Navy Strategic Systems Programs (cont'd)**

~~CONTROLLED UNCLASSIFIED INFORMATION~~


Navy (b)(1) 1.7(e)



Navy (b)(1) 1.7(e)




Navy (b)(1) 1.7(e)



3. Appendix B of the report provides the DoD IG's responses to specific House Armed Services Committee (HASC) questions regarding supply chain risk management. SSP has reviewed the responses and provides the following comments:

Navy (b)(1) 1.7(e)




~~CONTROLLED UNCLASSIFIED INFORMATION~~


**(U) Director, Navy Strategic Systems Programs (cont'd)**

~~CONTROLLED UNCLASSIFIED INFORMATION~~

Navy (b)(1) 1.7(e)



Navy (b)(1) 1.7(e)



~~CONTROLLED UNCLASSIFIED INFORMATION~~

## **(U) Sources of Classified Information**

---

(U) **Source 1:** Annex E, "Classified Critical Program Information (CPI) and Mission Critical Function/Mission Critical Component Data," in Trident II SWS PPP (Document classified SECRET)

Declassification Date: May 16, 2042

Generated Date: May 16, 2017

(U) **Source 2:** The National Defense Strategy, "Sharpening the American Military's Competitive Edge," January 19, 2018. (Document classified SECRET)

Declassification Date: January 19, 2043

Generated Date: January 19, 2018

## (U) Acronyms and Abbreviations

---

<b>DASN(RDT&amp;E)</b>	Deputy Assistant Secretary of the Navy for Research, Development, Test, and Evaluation
<b>DASN(S)</b>	Deputy Assistant Secretary of the Navy for Sustainment
<b>DCMA</b>	Defense Contract Management Agency
<b>GAO</b>	Government Accountability Office
<b>PPP</b>	Program Protection Plan
<b>SCRM</b>	Supply Chain Risk Management
<b>SSBN</b>	Ship Submersible Ballistic Nuclear
<b>SSP</b>	Strategic Systems Programs
<b>SWS</b>	Strategic Weapon System

## (U) Glossary

---

**(U) Application-Specific Integrated Circuit.** An integrated circuit that is custom-designed or custom-manufactured for a particular use.

**(U) Critical Component.** A component which is or contains information and communications technology, including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission-critical functions of an applicable system.

**(U) Criticality Analysis.** An end-to-end functional analysis performed by systems engineers to identify mission-critical functions and components. Criticality analysis includes identification of systems missions, decomposition into the functions to perform those missions, and traceability to the hardware, software, and firmware components that implement those functions. Criticality is assessed in terms of the impact of function or component failure on the ability of the component to complete the system missions.

**(U) Information and Communications Technology.** All categories of ubiquitous technology used for gathering, storing, transmitting, receiving, or processing information (for example, microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).

**(U) Integrated Circuit.** A set of micro-miniature electronic circuits fabricated on a single piece of semiconducting material.

**(U) Mission Critical Function.** Any function, the compromise of which would degrade the system effectiveness in achieving the core mission for which it was designed.

**(U) National Security System.** Any information system (or telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency, the function or use of which: (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapons system; or (5) is critical to the direct fulfillment of military or intelligence missions.

**(U) Program Protection Plan (PPP).** A risk-based, comprehensive, living plan to guide efforts for managing the risks to critical program information and mission-critical functions and components.

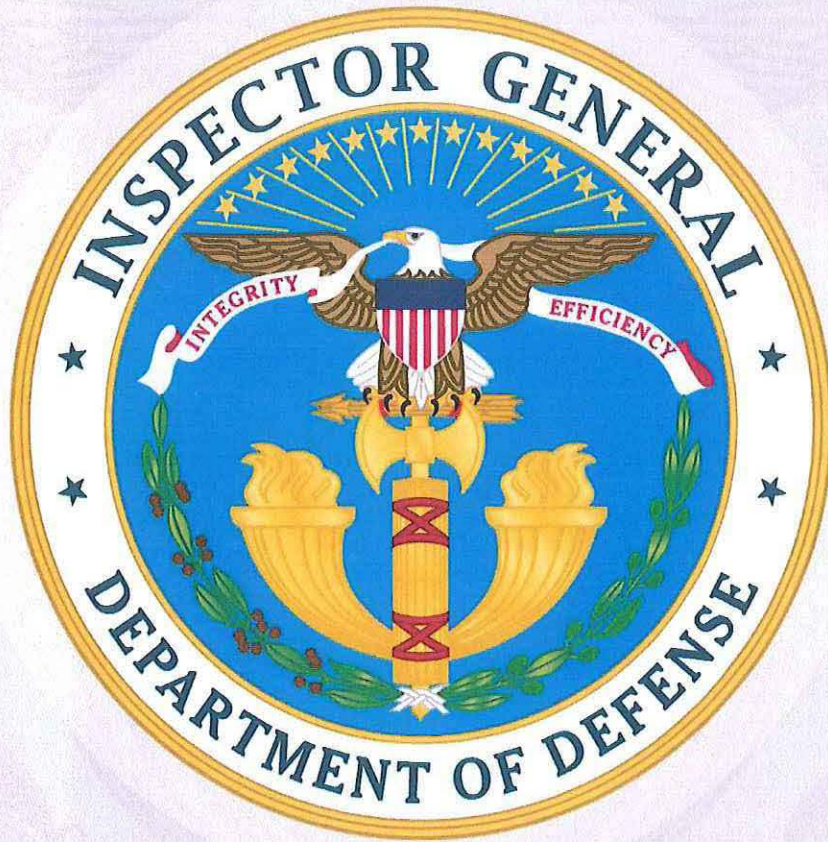


**(U) Supply Chain.** The linked activities associated with providing materiel from a raw material stage to an end user as a finished product or system, including design, manufacturing, production, packaging, handling, storage, transportation, mission operation, maintenance, and disposal.

**(U) Supply Chain Risk.** The risk that an adversary may sabotage, maliciously introduce an unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system.

**(U) Supply Chain Risk Management (SCRM).** A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the DoD's supply chain and developing mission strategies to combat those threats whether presented by the suppliers, the supplied product and its subcomponents, or the supply chain (for example, initial production, packaging, handling, storage, transport, mission operation, and disposal).

~~SECRET~~



~~SECRET~~

## **Whistleblower Protection**

### **U.S. DEPARTMENT OF DEFENSE**

*The Whistleblower Protection Ombudsman's role is to educate agency employees about prohibitions on retaliation and employees' rights and remedies available for reprisal. The DoD Hotline Director is the designated ombudsman. For more information, please visit the Whistleblower webpage at [www.dodig.mil/Components/Administrative-Investigations/DoD-Hotline/](http://www.dodig.mil/Components/Administrative-Investigations/DoD-Hotline/).*

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

**Congressional Liaison**

703.604.8324

**Media Contact**

public.affairs@dodig.mil; 703.604.8324

**For Report Notifications**

[www.dodig.mil/Mailing-Lists/](http://www.dodig.mil/Mailing-Lists/)

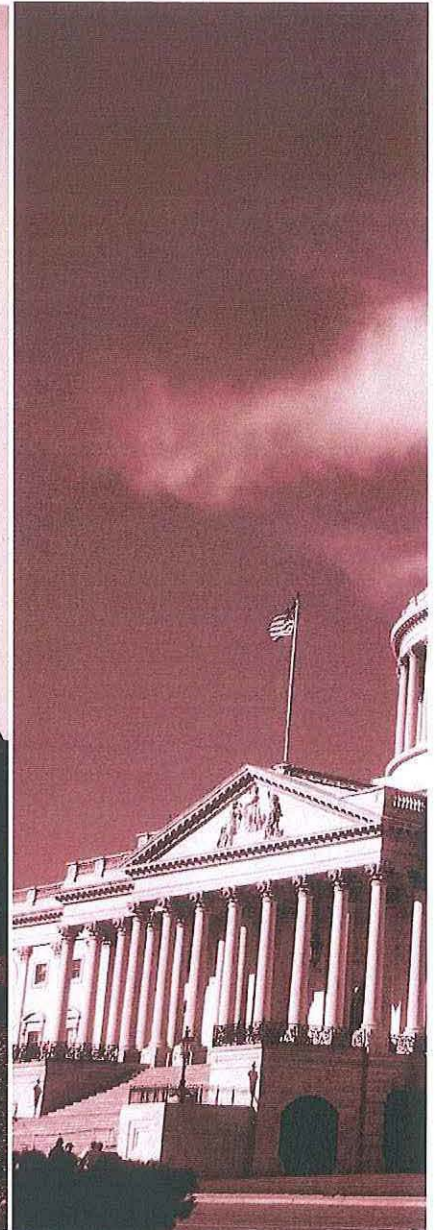
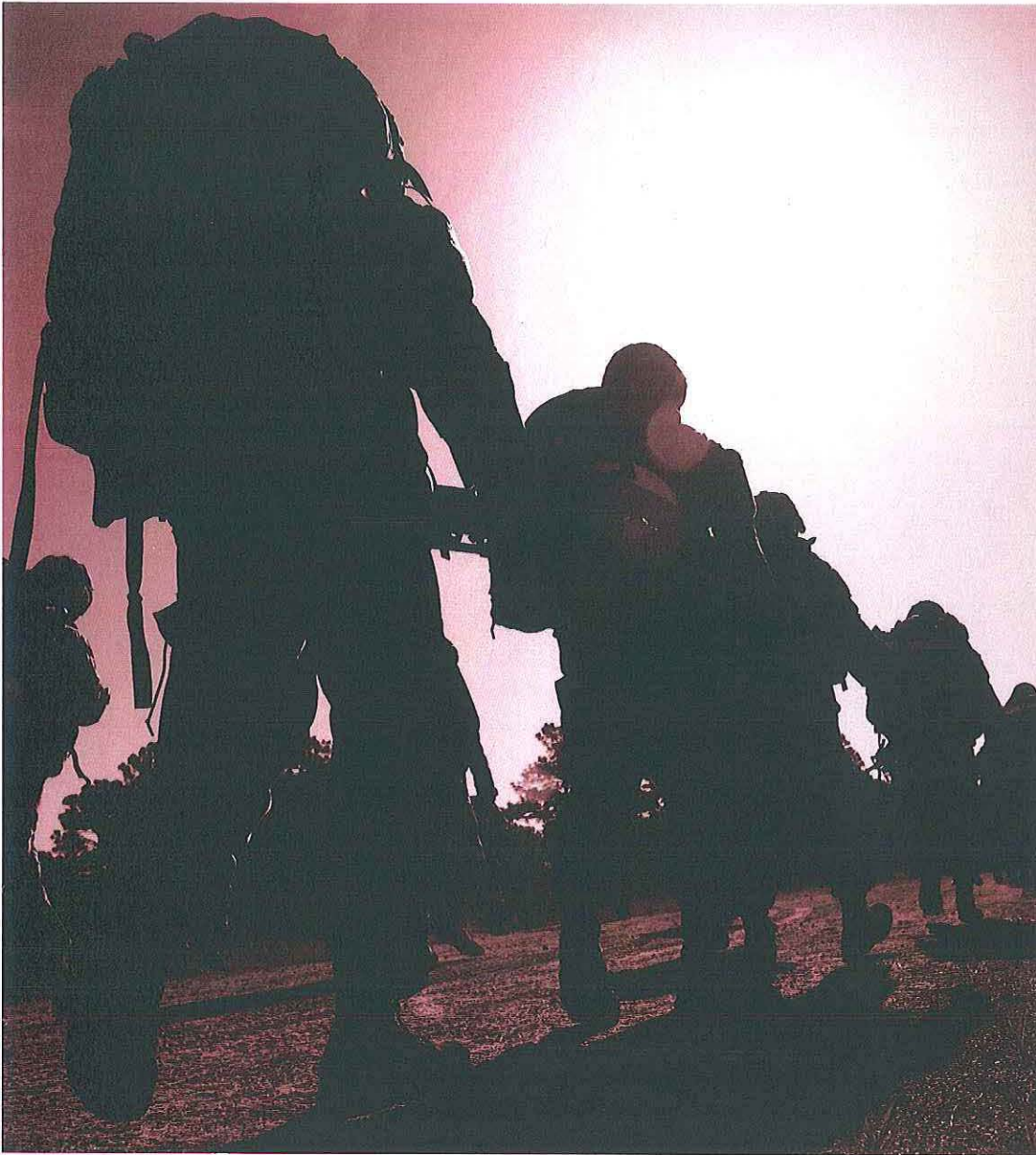
**Twitter**

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

**DoD Hotline**

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

~~SECRET~~



DEPARTMENT OF DEFENSE | OFFICE OF INSPECTOR GENERAL

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

~~SECRET~~