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

OCT 2 8 2016

Ref: 11-00211-F

SENT VIA EMAIL TO: saftergood@fas.org
Mr. Steven Aftergood
Federation of American Scientists
1725 DeSales Street NW, Suite 600
Washington, DC 20036

Dear Mr. Aftergood:

This is in response to your June 13, 2011, Freedom of Information Act (FOIA) request for a copy of report 11-INTEL-06. We received your request on June 14, 2011, and assigned it case number 11-00211-F.

The Office of the Deputy Inspector General for Intelligence and Special Program Assessments conducted a search and found the enclosed document responsive to your request. I determined that some redacted portions are exempt from release pursuant to 5 U.S.C. § 552 (b)(6), which pertains to information, the release of which would constitute a clearly unwarranted invasion of personal privacy. In addition, the National Security Agency (NSA) also reviewed the report and determined certain portions are exempt from release pursuant to (b)(3), information exempted from release by statute, in this instance, 50 U.S.C. § 3605, information dealing with NSA functions and information.

In view of the above, you may consider this to be an adverse determination that may be appealed to the Department of Defense, Office of Inspector General, ATTN: FOIA Appellate Authority, Suite 10B24, 4800 Mark Center Drive, Alexandria, VA 22350-1500. Your appeal, if any, must be postmarked within 90 days of the date of this letter and should reference the file number above. I recommend that your appeal and its envelope both bear the notation "Freedom of Information Act Appeal."

You may seek dispute resolution services and assistance with your request from the DoD OIG FOIA Public Liaison Officer at 703-604-9785, or the Office of Government Information Services (OGIS) at 877-684-6448, ogis@nara.gov, or https://ogis.archives.gov/. Please note that OGIS mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. However, OGIS does not have the authority to mediate requests made under the Privacy Act of 1974 (request to access one's own records).

If you have any questions regarding this matter, please contact the Department of Defense, Office of Inspector General FOIA Requester Service Center at 703-699-7498 or via email at foiarequests@dodig.mil.

Sincerely,

Mark Dorgan
Division Chief
FOIA, Privacy and Civil Liberties Office

Enclosure(s):
As stated

Report No. 11-INTEL-06
March 9, 2011

Inspector General

United States
Department *of* Defense

DEPUTY INSPECTOR GENERAL FOR INTELLIGENCE

(U) Assessment of Intelligence Community Whistleblower Protection Act Allegations

Derived From: ~~NSA/CSSM 1-52~~
Dated: January 8, 2007
Declassify On: ~~20320108~~

~~This document will not be released (in whole or in part) outside the Department of Defense without the prior written approval of the Inspector General of the Department of Defense.~~

(U) Additional Copies

(U) To request copies of the report, contact the Department of Defense Office of the Deputy Inspector General for Intelligence at (703) 604-8841 or DSN 664-8841.

(U) Suggestions for Audits and Evaluations

(U) To suggest or to request future audits and evaluations, contact the Office of the Deputy Inspector General for Intelligence by phone (703) 604-8800 (DSN 664-8800), by UNCLASSIFIED fax (703) 604-0045, or by mail:

ODIG-INTEL (ATTN: Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 703)
Arlington, VA 22202-4704

DEPARTMENT OF DEFENSE
hotline

To report fraud, waste, mismanagement, and abuse of authority.

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900
Phone: 800.424.9098 e-mail: hotline@dodig.mil www.dodig.mil/hotline

(U) Acronyms and Abbreviations

CACMB	Cryptographic Algorithm Configuration Management Board
CIS	Cryptographic Interoperability Strategy
CNSS	Committee on National Security Systems
COTS	Commercial Off The Shelf
ECDH	Elliptic-Curve Diffie-Hellman
ECMQV	Elliptic-Curve Menezes-Qu-Vanstone
FIPS	Federal Information Processing Standard
GOTS	Government Off the Shelf
IAD	Information Assurance Directorate
ICWPA	Intelligence Community Whistleblower Protection Act
NIST	National Institute of Standards and Technology
NSA/CSS	National Security Agency/ Central Security Service

MAR 09 2011

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

MEMORANDUM FOR: UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY AND LOGISTICS;
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE;
ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/CHIEF INFORMATION OFFICER;
COMMANDER, UNITED STATES SOUTHERN COMMAND,
DIRECTOR, NATIONAL SECURITY AGENCY

SUBJECT: (U) Assessment of Intelligence Community Whistleblower Protection Act Allegations (Report No. 11-INTEL-06)

(U) We are providing this report for your information and use.

(U) We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-[redacted] DSN 664-[redacted] or [redacted] at (703) 604-[redacted] DSN 664-[redacted] If you desire, we will provide a formal briefing on the results.

Patricia A. Brannin
Deputy Inspector General
for Intelligence

CC:

OFFICE OF THE SECRETARY OF DEFENSE

Inspector General, Joint Staff

OTHER DEFENSE ORGANIZATIONS

Inspector General, National Security Agency

CONGRESSIONAL COMMITTEES AND SUBCOMMITTEES, CHAIRMAN AND RANKING MINORITY MEMBER

Senate Subcommittee on Defense, Committee of Appropriations
Senate Committee on Armed Services
Senate Select Committee on Intelligence
Senate Committee on Homeland Security and Governmental Affairs
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Permanent Select Committee on Intelligence
House Committee on Oversight and Government Reform
House Subcommittee on National Security, Homeland Defense, and Foreign Operations, Committee on Oversight and Government Reform

Report No. 11-INTEL-06 March 9 , 2011

(U) Results in Brief: Assessment of Intelligence Community Whistleblower Protection Act Allegations

(U) What We Did

(U//~~FOUO~~) In response to a Department of Defense Inspector General Intelligence Community Whistleblower Protection Act complaint we investigated four allegations related to the Cryptographic Modernization Strategy.

(U) Why We Did It

(U//~~FOUO~~) The Department of Defense Inspector General is required by statute (Inspector General Act of 1978, as amended) to investigate all valid allegations that meet the requirements of "urgent concern" and originating within a Department of Defense intelligence agency. The results of these investigations are then reported to both the Secretary of Defense and Congress.

(U//~~FOUO~~) The Complainant, a National Security Agency employee, made allegations regarding four aspects of the National Security Agency's Cryptographic Modernization Program:

- (U//~~FOU~~) Information Assurance Leadership exceeded the scope of their authorities.

- (~~S//REL~~) Replacing a portion of the algorithmic suite for securing specific types of information (Suite B) with another algorithm represented moving from the strongest to the weakest ever fielded. Such modifications had "incumbent security flaws and operational weaknesses."

- (U//~~FOUO~~) There is no interoperability between what is directed and currently fielded equipment.

- (U//~~FOUO~~) Cost of development of new cryptography modernization system would be wasteful and prohibitively expensive.

(U) What We Found

(U//~~FOUO~~) We found the National Security Agency has operated a Cryptographic Modernization Strategy since 2000 in accordance with Presidential, National and Agency policies, regulations, and authorities. This program has been methodically moving forward, with some minor setbacks along the way.

(U//~~FOUO~~) We did not substantiate any of the Complainant's allegations.

(U) What We Recommend

(U) We have no recommendations stemming from this assessment.

(U) This page intentionally left blank

Table of Contents

(U) This page intentionally left blank

(U) Introduction

(U) Objective

(U//~~FOUO~~) This assessment addresses specific allegations filed by a National Security Agency (NSA) employee via the Intelligence Community Whistleblower Protection Act (ICWPA)[1] concerning NSA's development of the Cryptographic Interoperability Strategy (CIS)[2], an enterprise-wide approach for securing both classified and unclassified information.

(U) Background

(U) The DoD Office of the Inspector General (OIG) Hotline received a complaint from a NSA civilian employee on March 12, 2010. The employee requested the complaint be filed under the ICWPA. As required by ICWPA procedures, the Deputy Inspector General for Intelligence forwarded the complaint through the DoD OIG and the Secretary of Defense to Congress within the required timeframe.

(U) In addition, the complainant made an allegation of reprisal. The reprisal was investigated by the DoD OIG Civilian Reprisal Investigations. The reported reprisal investigation is issued under separate cover.

(U//~~FOUO~~) The complainant alleged the NSA's Information Assurance Directorate's (IAD) acquisition, development, and fielding of the CIS, which incorporates commercially available technology for securing information "will jeopardize future secure communications and gravely affect the use of fielded IAD technologies."

(U//~~FOUO~~) The complainant's allegations describe IAD leadership as being "set out on a strategic direction that can only be described as commercial interoperability at all costs." The complainant believes IAD leadership knowingly ignored key factors related to security, interoperability, and cost during the development of the CIS to reach a desired outcome.

(U) The allegations are:

- (U//~~FOUO~~) IAD leadership exceeded the scope of their authorities to develop the Suite B program;

[1] (U) See Appendix B for a discussion of the ICWPA process.
[2] (U//~~FOUO~~) See Appendix C for a discussion of the CIS, which is an initiative to create interoperability between government, international partners and first responders, and Suite B.

- ~~(S//REL~~) Replacing a portion of the CIS's algorithmic suite for securing specific types of information (Suite B) with another algorithm represents moving from the strongest to the weakest ever fielded. Additionally, the complainant alleged such modifications had "incumbent security flaws and operational weaknesses";

- (U//~~FOUO~~) There is no interoperability between what is directed in the CIS and currently fielded equipment; and

- (U//~~FOUO~~) Cost of development of new cryptography modernization system would be wasteful and prohibitively expensive due to the need to build new suites of communications equipment that can support the new algorithms.

(U//~~FOUO~~) The NSA IG conducted an audit regarding similar allegations prior to, and independent of the DoD IG assessment. The NSA IG audit, released on August 10, 2010, was unable to substantiate or disprove the allegations.

(U) This page intentionally left blank

(U) Finding. Unsubstantiated Allegations of Program Mismanagement

(U//~~FOUO~~) The complainant alleges IAD leadership exceeded their authorities when they "set out on a strategic direction that can only be described as commercial interoperability at all costs." The complainant alleges IAD leadership directed the IAD workforce to implement an algorithm within Suite B that would be moving from the strongest to the weakest, and thereby reducing security, while providing no interoperability between current fielded equipment and Suite B. According to the complainant, this would result in incurring unnecessary costs, all while "introducing grave risks to all NSA developed cryptographic products..." We did not substantiate these allegations.

(U) Program Authorities

(U) NSA derives its authorities to implement cryptographic changes to the national security systems from National Security Directive-42, which designates Director, NSA as National Manager for National Security Telecommunications and Information Systems Security.

(U//~~FOUO~~) As part of the NSA's responsibilities to secure national security systems and in response to tasking from national authorities, the NSA began developing a Cryptographic Modernization Roadmap in 2001 with the goal of upgrading and modernizing the DoD's cryptographic inventory.[3]

(U//~~FOUO~~) In accordance with national policy and in support of this effort, IAD, the NSA's office of primary responsibility for the Cryptographic Modernization Roadmap, developed an algorithm suite using National Institute of Standards and Technology (NIST)-approved commercial algorithms to secure certain types of sensitive and classified information.[4] [5] This suite of algorithms, known as Suite B, uses four algorithms to encrypt information, authenticate the data being sent, and ensure secure communications between the sender and receiver (key establishment) of a message.

(U//~~FOUO~~) Using the NIST-approved commercial algorithms in the development of Suite B represented a radical change for the NSA, as the NSA had traditionally developed and implemented solutions internally using classified algorithms. IAD leadership told us such a migration was essential as commercial solutions have caught up to government

[3] (U) See Appendix D for a discussion of the NSA's national authorities as they relate to cryptographic modernization.

[4] (U) See Appendix C for more information regarding Suite B and the Cryptographic Interoperability Strategy.

[5] (U) See Appendix E for the IAD Organizational Chart.

solutions in terms of capabilities, and using commercial solutions assists the NSA meeting its customers' requirements without sacrificing security. IAD leadership also told us using commercial solutions provided a more comprehensive security posture and "defense in depth" throughout the user, system, and network levels.

(U) Suite B Algorithm Selection and Testing

(U//~~FOUO~~) We assessed the process for the selection and testing procedures of the algorithms, not the actual strength of the algorithms. During the original algorithm selection for Suite B, IAD chose both Elliptic Curve Menezes-Qu-Vanstone (ECMQV) and Elliptic Curve Diffie Hellman (ECDH) algorithms to serve as the suite's key establishment component. Both ECMQV and ECDH are NIST approved public algorithms the NSA deemed appropriate to serve as Suite B's key exchange algorithm.

(U//~~FOUO~~) In 2007, IAD leadership made the decision to drop ECMQV from Suite B, electing to solely use ECDH as the Suite B key exchange algorithm, mainly due to interoperability concerns and an unforeseen lack of commercial interest stemming from potential patent issues related to ECMQV. As a result, ECDH was implemented as the Suite B key exchange algorithm because "interoperability is the Suite B driver."

(U//~~FOUO~~) Since ECDH's selection to be the sole key exchange component of Suite B, at least one commercially developed product, the Harris RF-310M-HH tactical radio has been NSA certified for field use implementing Suite B components. IAD leadership confirmed they do not currently have a formal procedure established for implementing commercial off the shelf (COTS) solutions using Suite B or Suite B components into products, but are in the process of developing a COTS implementation procedure. However, in the absence of a formal COTS methodology, IAD leadership followed the approved implementation methodology outlined in NSA/CSS Policy Number 3-9 (Cryptographic Modernization Initiative Requirements for Type I Cryptographic Products[6]). A key component of the policy is: "All development activities shall document and receive Cryptographic Algorithm Configuration Management Board (CACMB) approval of their planned algorithm use."

(U//~~FOUO~~) NSA established the CACMB in 2001 to "Establish processes for program managers to follow in proposing algorithm use and registering algorithms and specifications." Among its other duties the CACMB is responsible for reviewing and approving algorithms to support the "corporate goals in crypto-modernization, interoperability, and releasability."[7]

[6] (U//~~FOUO~~) Type I Cryptographic products are those certified by NSA for securing classified and sensitive U.S. Government information when appropriately keyed, and contain approved NSA algorithms.

[7] (U//~~FOUO~~) A complete list of CACMB tasks can be found in Information Systems Security Organization Regulation No. 11-04, as well as the CACMB Charter.

(U//~~FOUO~~) The CACMB is overseen by the IAD Senior Cryptographic Evaluation Authority (a NSA senior technical director), who is responsible to the Director of IAD to provide IAD approval of cryptographic algorithms; and consists of representatives from NSA security, IAD research, solutions, operations, and technical support, as well as, representation from the United Kingdom.The CACMB is "the authoritative source for implementation on, and approval of algorithm usage including modes, specifications, and reference implementations."The CACMB issued an initial algorithm approval procedure in September 2004, further clarifying the procedure in May 2009. The CACMB is also in the final stages of approving CACMB-100, "Cryptographic Algorithm Guidance," which specifies the use of ECDH as the Suite B key exchange algorithm.

(U//~~FOUO~~) The Senior Cryptographic Evaluation Authority told us, and we confirmed through independent review of documentation, that both IAD's Vulnerability Analysis and Operations Group and Custom Solutions Group approved ECDH as the Suite B key exchange algorithm. The decision to use ECDH was highlighted in the IAD approved and released Cryptographic Interoperability Strategy Implementation Plan Version 2.0, to support the adoption of commercially available Suite B products and advance the adoption of Committee of National Security Systems (CNSS) Policy Number 15 (CNSSP 15), National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems, dated March 29, 2010.

~~(S//REL)~~ NSA CSS (b)(3), 50 USC § 3605 [redacted] To ensure Suite B's integrity, ECDH would never be employed alone. In order to provide the necessary level of information assurance, ECDH must be incorporated with the other Suite B component algorithms and approved implementation protocols.[8]

(U//~~FOUO~~) Additionally, there has been an informal process at NSA for nearly 20 years between the IAD Office of Research and the Office of Cryptographic Services for algorithm evaluation, to include the evaluations of ECDH and ECMQV. After the CACMB was established, the process was augmented to include the CACMB as an additional layer of algorithm review and approval.

~~(S//REL)~~ The cryptographic experts from the Office of Research and the Office of Information Assurance Infrastructure Development and Operations wrote a draft decision paper in 2007 comparing ECDH to ECMQV. The draft decision paper mirrored the IAD leadership's decision to implement ECDH over ECMQV in Suite B; the IAD Technical Director's decision was made before the draft decision paper was finalized. NSA CSS (b)(3), 50 USC § 3605 [redacted]

[8] (U//~~FOUO~~) CNSSP 15 further elaborates this point in stating "Achieving the requisite level of protection is dependent on more than just employing cryptographic algorithms. The quality of the implementation and supporting public key and key management infrastructures are equally important."

NSA/CSS (b)(3), 50 USC § 3605 [redacted] After an in-depth analysis of both ECMQV and ECDH, the authors concluded ECDH was the most viable algorithm for Suite B's key exchange component.

(U//~~FOUO~~) IAD is coordinating three ongoing pilots strictly using COTS products with ECDH based Suite B using real world applications to identify issues with the COTS products and the CIS. Once the pilots conclude, the NSA will further refine certification and accreditation methodology for using commercial solutions for classified information assurance (also known as COTS for Classified). These pilots are also attempting to address backwards compatibility with fielded legacy equipment.

(U) Interoperability Concerns

(U//~~FOUO~~) The complainant alleges "There is no interoperability between what is being directed in the CIS and what is being implemented in the field." The RF-310M-HH tactical radio is the only device currently certified to use Suite B components. Major vendors, to include IBM, Microsoft, Sun Microsystems, Oracle, Cisco, Harris, Research in Motion, and Cygnacom, are implementing Suite B into their products. Furthermore, IAD continues to use various pilot programs to test and resolve interoperability issues. Due to its current development status, the implementation of Suite B employing ECDH or a commensurate suite of NSA-approved cryptographic algorithms is not mandated until October 1, 2015.

(U) Program Budget

(U//~~FOUO~~) The complainant raised concerns regarding the funding associated with the development of ECDH as the key exchange component of Suite B, both in terms of product development and key management infrastructure support. The complainant states IAD will potentially waste as much as $250 million on the CIS/Suite B transition and an additional $125 million in the future on key management support. We determined that these figures were represented as a worst case scenario. Actual costs cannot be determined as the program is still in development and IAD, through its testing methodology and pilots, is taking steps to mitigate costs. At this time, the projected costs are $92 million through fiscal year 2015.

(U/~~FOUO~~) IAD budget personnel provided us budget documentation supporting the development of the Suite B program. We found an established and approved budget in place for Suite B development through Suite B's mandated implementation date as specified by CNSSP 15. The funding documents show the actual and planned funding for the Suite B initiative by each fiscal year through FY 2017 and how each component of IAD is supporting the Suite B initiative.

(U) Additionally, a senior budget official in Office of the Assistant Secretary of Defense for Networks & Information Integration confirmed receiving briefings related to Suite B policies and implementation.

(U) Conclusion

(U//~~FOUO~~) We determined there was no evidence to support the allegations that IAD leadership ignored concerns regarding interoperability, cost, or security. We also determined IAD leadership did not exceed the scope of their authority in their decision to implement ECDH over ECMQV as the key establishment algorithm in Suite B.

~~(S//REL TO USA, FVEY)~~ We did not find definitive evidence to support the allegation that replacing ECMQV with ECDH as the Suite B key exchange algorithm represented a move from the strongest to the weakest key exchange ever fielded, or created incumbent security flaws and operational weaknesses. Our assessment did show that the people with the right authorities are clearly following established program development protocols within the scope of their authorities to certify the Suite B algorithms. While there is not currently a formal testing methodology for COTS products, IAD conducted its ECMQV/ECDH algorithm research using existing authorities in accordance with approved CNSS, NIST, and IAD internal guidance and specifications. This approach was based on more than 20 years of proven government developed product vetting and testing of Type I cryptographic equipment. Implementing NSA IG's report number AU-0001-10 recommendation for the development and implementation of a formal requirements protocol for COTS products similar to NSA/CSS Policy 3-9 will provide the appropriate level of security assurance to COTS products that GOTS products currently possesses.

(U//~~FOUO~~) Based on our review and in conjunction with IAD budget and development personnel, the budgetary documentation and CIS pilots demonstrate IAD leadership is acting within the scope of their authority and has not violated the budgetary guidelines approved for the Suite B initiative.

(U//~~FOUO~~) At this juncture, we cannot determine what the overall cost for the CIS/Suite B implementation including ECDH will be as the transition has yet to occur. IAD leadership is attempting to mitigate these costs through policy development, pilot programs, and engagement with stakeholders throughout the development process.

(U) Observations

(U) IAD Organizational Culture

(U) Through interviews of IAD senior leadership and functional-level workforce, we found that some IAD employees have strong opinions concerning the implementation of Suite B, but IAD management made decisions within the scope of their authorities. Also, some members of the workforce do not know or understand all of the aspects of the bigger IAD strategy. Since using a COTS strategy represents such a radical departure from NSA's traditional acquisition approach, the IAD leadership believes some of these employees may feel threatened by new approaches, such as COTS, where development applies risk management rather than risk aversion. To mitigate these concerns, IAD leadership held multiple town hall meetings, online discussion blogs, question and answer sessions, and one-on-one meetings for concerned employees.

(U) Approving Formal Cryptographic Algorithm Guidance

(U//~~FOUO~~) The CACMB-100 has been in the review and final coordination process since at least April 2010. Publishing the CACMB-100 will provide IAD's program managers definitive guidance related to implementing CNNSP 15 and the CIS, and better define the NSA's testing methodology for cryptographic products.

(U) Appendix A. Scope and Methodology, Prior Coverage

(U) Scope and Methodology

(U//~~FOUO~~) Our assessment was performed from July 2010 to November 2010 in accordance with the "Quality Standards for Inspections." We reviewed supporting documentation and briefings regarding the CIS Team, the Implementation Plan, the Marketing Plan, policies and standards (draft and final), and information related to the CIS objectives and milestones. We interviewed CIS/Suite B subject matter experts from NSA and the Office of the Assistant Secretary of Defense for Networks & Information Integration. Given the extensive documentation provided, we determined we had sufficient information to address the ICWPA allegations and did not need to interview personnel from the Office of the Under Secretary of Defense for Intelligence, the Under Secretary of Defense for Acquisition, Technology, and Logistics or U.S. Southern Command.

(U) We interviewed the complainant concerning the allegations.

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

(U) We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our assessment objectives.

(U) Prior Coverage

(U) NSA Inspector General Report

(U) "Audit Report on the Cryptographic Interoperability Strategy (CIS)/Suite B", NSA OIG Report No. AU-10-0001, August 20, 2010

~~(S//REL)~~ The NSA Inspector General received whistleblower allegations in August and October of 2009 regarding the CIS known as Suite B. The NSA Inspector General categorized the allegations as:

- Lack of radio interoperability,
- Lack of CIS customer interest, and
- Elliptic Curve Diffie-Hellman (ECDH) key exchange algorithm is weaker than an alternative algorithm.

(U//~~FOUO~~) The NSA OIG recommended IAD implement a process to document the evaluation results of publicly available cryptographic algorithms, similar to the procedures followed for internally generated algorithms; and document the management decision for selecting ECDH for Suite A and Suite B.

(U//~~FOUO~~) IAD management concurred with the NSA IG recommendations and implemented a plan of documenting the evaluation results and management decisions on NSA Staff Processing Forms. The forms will then be maintained in a repository at the Cryptographic Algorithm Configuration Management Board.

(U) Appendix B. The Intelligence Community Whistleblower Protection Act

(U) The Intelligence Community Whistleblower Protection Act (ICWPA) is codified in the Inspector General (IG) Act of 1978 [as amended] (5 U.S.C. App. Inspector General Act of 1978 § 8H). The ICWPA provides employees of the four defense agencies in the Intelligence Community (National Reconnaissance Office, Defense Intelligence Agency, National Security Agency, and National Geospatial Intelligence Agency) a secure conduit for transmitting complaints or information of urgent concern related to classified material to Congress. The ICWPA defines an urgent concern as one of the following:

i. (U) A serious or flagrant problem, abuse, violation of law or Executive order, or deficiency relating to the funding, administration, or operations of an intelligence activity involving classified information, but does not include differences of opinions concerning public policy matters.

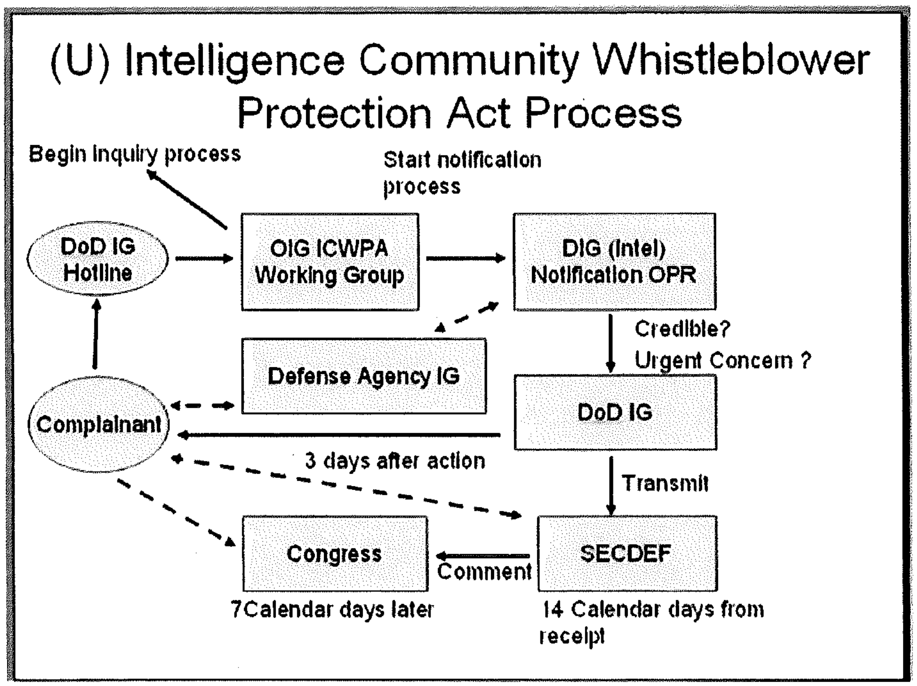
ii. (U) A false statement to Congress, or a willful withholding from Congress, on an issue of material fact relating to the funding, administration, or operation of an intelligence activity.

iii. (U) An action, including prohibited personnel actions, constituting reprisal or threat of reprisal, which prohibited in response to an employee's reporting an urgent concern in accordance with the ICWPA.

(U) The IG Act of 1978 has most recently been amended by the 2010 Intelligence Authorization Act (Public Law 111-259), which codified the four defense agencies in the DoD Intelligence Community as designees of the DoD OIG with regard to the whistleblower section of the IG Act of 1978, as amended (Section 8H). This amendment did not fundamentally change the previous reporting structure.

(U) Employees and contractors of the four defense agencies in the DoD who believe their issue meets the definitions of an urgent concern and credibility can report to their respective agency's IGs or directly to the DoD OIG Hotline. The defense intelligence agency IGs have 7 calendar days to report the information to the DoD OIG, who in turn has 14 calendar days to determine whether the complaint or information appears credible and is of urgent concern. If the DoD OIG determines that the complaint or information appears credible and of urgent concern, then the DoD OIG shall transmit the complaint or information to the Secretary of Defense. The DoD OIG may also forward comments on the complaint or information to the Secretary of Defense. The Secretary of Defense, upon receiving the information from the DoD IG, has 7 calendar days to send a transmittal letter to the Congressional intelligence committees along with any additional information. Within 3 days after each action is complete the DoD OIG is required to submit a notification to the complainant. Figure 1 depicts the ICWPA process.

(U) Figure 1. The ICWPA Process



(U) Intelligence Community Whistleblower Protection Act Process

(U) Appendix C. Cryptographic Interoperability Strategy/Suite B

(U) The Cryptographic Interoperability Strategy Background

(U) Due to the increased need for interoperability, the CIS was conceived to increase assured rapid sharing of information both within the U.S. and between the U.S. and her partners. The CIS centers on a common suite of public standards, protocols, algorithms and modes known as the Secure Sharing Suite. Implementation of the CIS will facilitate development of a broader range of secure cryptographic products that will be available to a wide customer base. Some operational examples include enabling the U.S. Government to securely share intelligence information with state and local first responders and for war fighters to securely share information on the battlefield with non-traditional coalition partners.

(U) The secure sharing of information, especially for the tactical user, creates the need for widespread cryptographic interoperability and NSA-approved information assurance products meeting appropriate security standards to protect classified information at the SECRET level. These needs will only be satisfied with widely available and affordable NSA-approved information assurance solutions. NSA has initiated three efforts to address these needs:

- The CIS;

- Layered COTS products meeting a more robust set of security standards to protect information up to the SECRET level; and

- Expanding the use of Government Off the Shelf (GOTS) products that meet a revised set of security standards to protect information up to the SECRET level. As part of the overall strategy, NSA is developing a process, known as GOTS for Secret. This process will allow commercial vendors with NSA-certified Type I cryptographic products to develop product variants that implement Suite B cryptography and meet a revised set of NSA's security standards for protecting information up to the SECRET level. When these products do not contain any classified algorithms or technology, the handling and accountability requirements will be less stringent than for a Controlled Communications Item,[9] thereby allowing for wider distribution of communication systems.

(U) The NSA-CIS team is composed of subject matter experts from across the IA mission, including Research, NSA/CSS Commercial Solutions Center, International

[9] (U) The IAD Manual defines a Controlled Communications Item as Secure telecommunications or information handling equipment, or associated cryptographic component items that is unclassified but governed by a special set of control requirements.

Affairs, and the IAD Groups.[10] To achieve the Strategy, NSA is working to influence international standards groups as well as national policies for securing National Security Systems. The use of selected public cryptographic standards and protocols and Suite B is the core of CIS.

(U) The CIS involves increasing secure sharing through:

- incorporating Suite B in commercial standards and protocols, which will create a new market place;
- identifying commercial infrastructure provider(s);
- persuading vendors to build Suite B products;
- influencing customers to adopt CIS;
- evolving NSA's infrastructure to support CIS;
- updating policy and doctrine to reflect Suite B usage; and
- evolving IAD processes (testing, evaluations, certification, CACMB, etc).

(U) The Commercial Solutions Partnership Program is being developed between the NSA and the commercial world using publically available COTS information assurance products to protect information up to the SECRET level by layering products to increase security.

(U) The NSA has adopted a number of public protocols[11] which are recognized worldwide. These protocols are being built into the CIS Internet Protocol Security Minimum Essential Interoperability Requirements[12] strategy to further enhance interoperability. These protocols include:

- Internet Protocol Encryption;
- Web Traffic, Application Communication, Virtual Private Networks; and
- Secure Electronic Mail.

[10] (U) We found NSA has been providing CIS and Suite B details on both its public NSA.gov website as well as its Joint Worldwide Intelligence Communications System (JWICS) website, www.iad.nsa.ic.gov since 2005. These websites provide an in-depth view of CIS background, NSA goals problems and strategies. The websites discuss the CIS standards, protocols, and public algorithms used.

[11] (U) A protocol is a set of rules and formats, semantic and syntactic, permitting information systems to exchange information.

[12] (U) Internet Protocol Security Minimum Essential Interoperability Requirements are being implemented in government equipment to foster interoperability with commercial industry. NSA has developed specification documents to support the Commercial Interoperability Specification Suite B Strategy by providing commercial IPSec network product producers and traditional government network encryptor vendors with minimum interoperability requirements.

(U) Algorithms and Suite B

(U) Over the past 35 years, public key cryptography has become a mainstay for secure communications over the internet and throughout many other forms of communications. It provides the foundation for both key management and digital signatures. In key management, public key cryptography is used to distribute the secret keys used in other cryptographic algorithms. For digital signatures, public key cryptography is used to authenticate the origin of data and protect the integrity of that data. For the past 25 years, internet communications have been secured by the first generation of public key cryptographic algorithms developed in the mid-1970's.

(U) At their inception, these public key techniques revolutionized cryptography. Over the last 25 years, new techniques have been developed that offer both better performance and higher security than these first generation public key techniques. The best assured group of new public key techniques is built on the arithmetic of elliptic curves. At current security levels elliptic curves do not offer significant benefits over existing public key algorithms, however, as one scales security upwards over time to meet the evolving threat posed by eavesdroppers and hackers with access to greater computing resources, elliptic curves begin to offer dramatic savings over the old, first generation techniques.

(U) Invented around 1975, the two main first generation public key algorithms used to secure the internet today are known as Rivest, Shamir and Adleman and Diffie-Hellman. Both algorithms are based on the use of elementary number theory. The security of the two schemes, though formulated differently, are closely related. Both algorithms have been subject to intense scrutiny since their invention. Over the years until the early 1990's, there have been many attempts to break the algorithms with specialized attack algorithms. There have also been several efforts aimed at designing theoretical special purpose computers that would implement the existing attack algorithms far faster than general computing resources.

(U) Since their use in cryptography was discovered in 1985, elliptic curve cryptography has also been an active area of study in academia. The Rivest, Shamir and Adleman and Diffie-Hellman algorithms slowly succumb to increasingly strong attack algorithms, while elliptic curve cryptography has remained at its full strength since it was first presented in 1985.

(U//~~FOUO~~) Suite B is a suite of four algorithms that will be used in concert in a cryptographic system to assure Confidentiality, Integrity, and Authentication of information that is classified SECRET and below. These algorithms have a high risk of loss or exposure, but are required for interoperability with commercial products. Figure 2 depicts the algorithms that comprise Suite B.

(U) Figure 2. Description of Suite B algorithm components.

(U)

	Definition	Algorithm	Required Size	Regulatory Document
Encryption (Confidentiality)	The process of changing plaintext into ciphertext for the purpose of security or privacy.	Advanced Encryption Standard	Keys sizes of 128 and 256 bits	Federal Information Processing Standards (FIPS) PUB 197
Key Exchange	Process of exchanging public keys (and other information) in order to establish secure communications.	The Ephemeral Unified Model and the One-Pass Diffie Hellman (referred to as ECDH)	Curves with 256 and 384- bit prime moduli	NIST Special Publication 800-56A
Digital Signature (Authentication)	Cryptographic process used to assure data object originator authenticity, data integrity, and time stamping for prevention of replay.	Elliptic Curve Digital Signature Algorithm	Curves with 256 and 384- bit prime moduli	FIPS PUB 186-3
Hashing (Integrity)	The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.	Secure Hash Algorithm	SHA-256 and SHA-384	FIPS PUB 180-3

(U) Figure 2. Suite B component algorithms as described in CNSSP-15. (U)

(U) Appendix D. National Policies related to the Cryptographic Interoperability Strategy/Suite B

(U//~~FOUO~~) We found a number of policies and significant events directly tied to the algorithm selection methodology for securing national security systems. These policies and events generally fall into one of two categories; those at the national level providing cryptographic strategic direction and specific agency responsibilities; and those at NSA describing operational development and implementation. This is a compilation of the most significant national level policies.

(U) National Security Directive-42 designates Director, NSA as National Manager for National Security Telecommunications and Information Systems Security. In this capacity, Director, NSA acts as the focal point for cryptography related to national security systems, conducts and approves research for securing national security systems, and reviews and approves all standards related to national security systems.

(U//~~FOUO~~) More recently, and in response to tasking from the Defense Resource Board,[13] the Cryptographic Modernization Working Group developed the Cryptographic Modernization Roadmap in 2001. The goal was to establish an enterprise-wide strategy for the DoD to upgrade its current inventory of cryptographic products and systems and the supporting key management infrastructure. The Roadmap places overall responsibility for the cryptographic modernization on the NSA, to include the NSA "retain(ing) responsibility for defining the security criteria for the DoD cryptographic inventory."

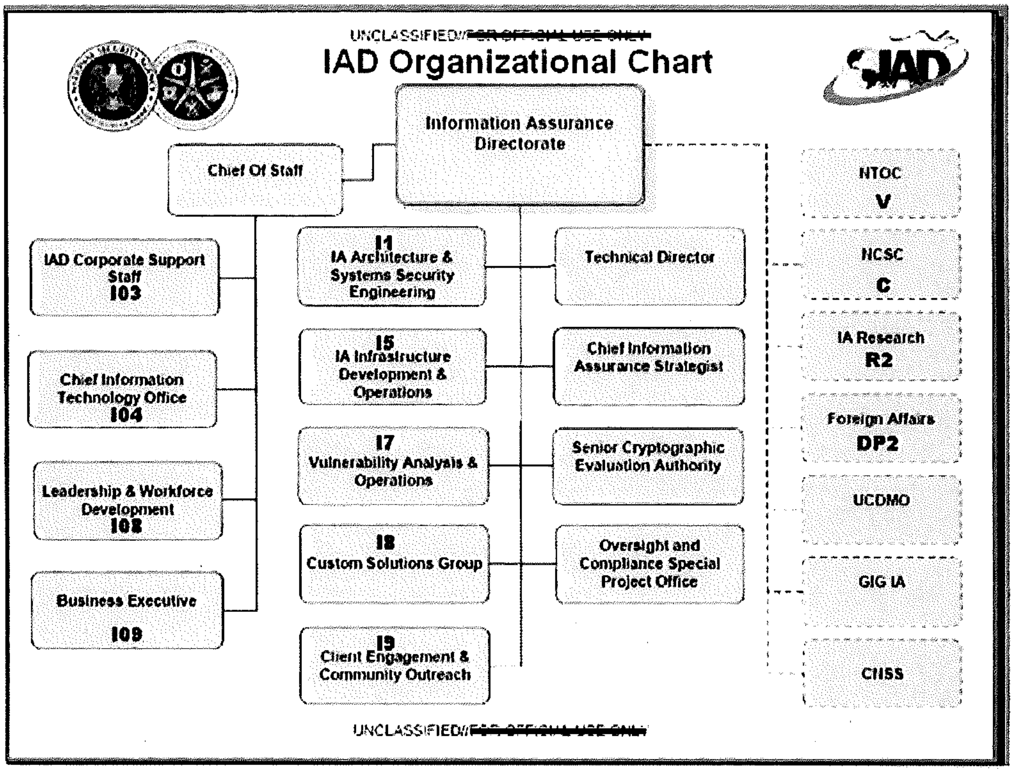
(U//~~FOUO~~) The CNSS also provides cryptographic guidance at the national level. Chaired by the Assistant Secretary of Defense for Network and Information Integration/DoD Chief Information Officer, and consisting of representatives or observers from 32 U.S. Government organizations, the CNSS prescribes national policies and directives related to national information assurance.

(U//~~FOUO~~) The CNSS issued specific guidance providing the responsibilities and list of approved algorithms in securing National Security Systems in CNSSP 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems, dated March 29, 2010. CNSSP 15 defines the algorithms comprising Suite B and states ECDH is the key establishment algorithm approved by both NSA and the CNSS for SECRET and TOP SECRET information.

[13] (U) The Defense Resource Board is chaired by the Deputy Secretary of Defense, and includes the Chairman of the Joint Chiefs of Staff, the Director, Program Analysis & Evaluation, as well as the Service Secretaries, Vice Chairman of the Joint Chiefs of Staff, and the Under Secretaries of Defense for Acquisition & Technology, Policy, Comptroller, and Personnel & Readiness.

(U//~~FOUO~~) CNSSP 15 also directs Director, NSA to assist in the selection of cryptographic algorithms, develop Suite B management guidance, as well as to "ensure that the CNSS is able to fulfill its roles and responsibilities." NSA's principle member to the CNSS is the IAD.

(U) Appendix E. Information Assurance Directorate Organizational Chart



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

IAD Organizational Chart

Information Assurance Directorate

Chief Of Staff

IAD Corporate Support Staff I03

Chief Information Technology Office I04

Leadership & Workforce Development I08

Business Executive I09

I1 IA Architecture & Systems Security Engineering

I5 IA Infrastructure Development & Operations

I7 Vulnerability Analysis & Operations

I8 Custom Solutions Group

I9 Client Engagement & Community Outreach

Technical Director

Chief Information Assurance Strategist

Senior Cryptographic Evaluation Authority

Oversight and Compliance Special Project Office

NTOC V

NCSC C

IA Research R2

Foreign Affairs DP2

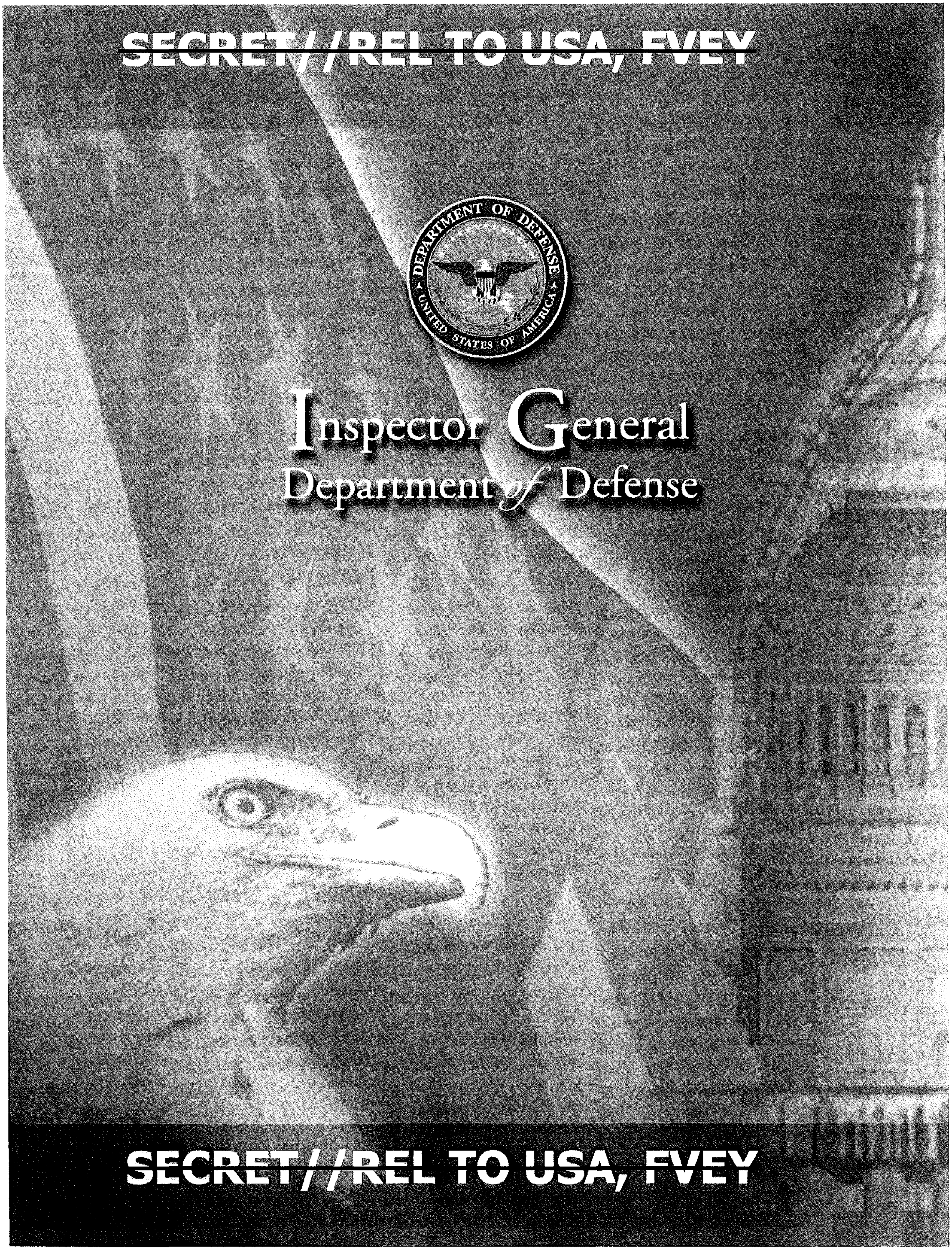
UCDMO

GIG IA

CNSS

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

(U) This page intentionally left blank



Inspector General
Department of Defense