DEPARTMENT OF DEFENSE
OFFICE OF FREEDOM OF INFORMATION
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

DEC 23 2015

Ref: 15-F-1206

Mr. Stephen Aftergood
Federation of American Scientist
1725 DeSales Street, NW
Suite 600
Washington, DC 20036

Dear Mr. Aftergood:

This is the final response to your enclosed May 20, 2015 Freedom of Information Act (FOIA) request for a copy "of a recent (2015) report to Congress from the Under Secretary of Defense (Intelligence) concerning the Department's plans to adopt continuous evaluation (CE) and Insider Threat capabilities within the Department of Defense." Your request was received in this office on May 20, 2015 and assigned FOIA case number 15-F-1206. We ask that you use this number when referring to your request.

The Office of the Under Secretary of Defense for Intelligence, a component of the Office of the Secretary of Defense, conducted a search of their records systems and provided the enclosed nine-page document; determine to be responsive to your request. This document is appropriate for release without excision. This constitutes a full grant of your request.

This action closes your request with this office. There are no assessable fees associated with this response in this instance.

Sincerely,

for Adrienne P. Santos
Stephanie L. Carr
Chief

Enclosure:
As stated

UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

INTELLIGENCE

APR 10 2015

The Honorable William M. "Mac" Thornberry
Chairman
Committee on Armed Services
US House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Section 1628 of the National Defense Authorization Act for Fiscal Year 2015, Public Law 113-291, directs the Secretary of Defense to provide a report on the Department's plans to adopt continuous evaluation (CE) and Insider Threat capabilities within the Department of Defense (DoD).

The requested report is attached. DoD is moving forward with the development of its insider threat and personnel security reform efforts, to include CE. The Department recognizes the magnitude and complexity of these challenges, the need for multi-agency solutions, and is marshalling needed resources.

My staff will provide additional details upon request. Similar letters are being sent to the President of the Senate, Speaker of the House, and the other congressional defense committees.

Sincerely,

Michael G. Vickers

Enclosure:
As stated

cc:
The Honorable Adam Smith
Ranking Member

Report on DoD Plans to Adopt Continuous Evaluation (CE) and Insider Threat Capabilities within the Department of Defense (DoD)

(a) REPORT REQUIRED. The Secretary of Defense shall submit to Congress a report on the plans of the Department to address:

(1) the adoption of an interim capability to continuously evaluate the security status of the employees and contractors of the Department who have been determined eligible for and granted access to classified information by the Department of Defense Central Adjudication Facilities;

(U//FOUO) The DoD currently has two capabilities to continuously evaluate the security status of DoD employees and contractors determined eligible for and granted access to classified information. DoD is enhancing the throughput capacity of its existing Automated Continuing Evaluation System (ACES) (which conducts point-in-time records checks) to "pull" data from trusted data sources, while concurrently developing the ACES Next Generation (ACES NextGen) "push" capability (where relevant updated information is automatically pushed to the system without additional queries). This approach enables the Department to leverage the CE efficiencies and timeliness of ACES NextGen while sustaining ACES as an efficient and cost-effective means for retrieving more detailed records.

(2) the use of an interim system to assist in developing requirements, lessons learned, business rules, privacy standards, and operational concepts applicable to the objective automated records checks and continuous evaluation capability required by the strategy for modernizing personnel security;

(U//FOUO) The Department is directing multiple pilots and concept demonstrations using both "push" and "pull" capabilities to conduct CE on approximately 100,000 military, civilian and contractor personnel. Concurrently, DoD has several analytic efforts underway to evaluate these efforts, including evaluating data sources, business rules, thresholds, processes and procedures. DoD will compare ACES checks to ACES NextGen results and Secret periodic investigations to inform the program's way ahead. The intent is to develop a business case for ultimately replacing Tier 3(i.e., Secret and Confidential) periodic reinvestigations with CE.

(3) the engineering for an interim system and the objective automated records checks and continuous evaluation capability for initial investigations and reinvestigations required by the strategy for modernizing personnel security to support automation-assisted insider threat analyses conducted across the law enforcement, personnel security, human

resources, counterintelligence, physical security, network behavior monitoring, and cybersecurity activities of all the components of the Department of Defense, pursuant to Executive Order 13587;

(U//FOUO) The DoD Insider Threat Management and Analysis Center (DITMAC) will leverage the extensive investment in the Department's CE capability currently being developed by the Defense Manpower Data Center (DMDC). Additionally, the DITMAC will leverage and integrate relevant counterintelligence, security, cybersecurity, human resources, and law enforcement information to identify, analyze, counter, and mitigate the insider threat. The DITMAC will recommend action as appropriate through a multifunctional team composed of law enforcement, mental health, counterintelligence, security, human resources, cybersecurity, and legal personnel.

(4) how competitive processes and open systems designs will be used to acquire advanced commercial technologies throughout the life cycle of the objective continuous evaluation capability required by the strategy for modernizing personnel security;

(U//FOUO) The Defense Manpower Data Center (DMDC), which is responsible for both ACES and ACES NextGen, will establish a formal program management office (PMO) for CE in late FY15. The CE PMO will follow federal and DoD acquisition policy to maximize open systems designs and competitive processes, as appropriate. For example, ACES NextGen is a Government-owned Off-the-Shelf system with an open system design that provides the Department with the flexibility to adjust business rules, the agility to interoperate with diverse systems, and the plasticity to integrate with new data sources as needed. The CE PMO will competitively negotiate data contracts to ensure flexibility and scalability required to align with changing mission priorities.

(5) how the senior agency official in the Department of Defense for insider threat detection and prevention will be supported by experts in counterintelligence, personnel security, law enforcement, human resources, physical security, network monitoring, cybersecurity, and privacy and civil liberties from relevant components of the Department and experts in information technology, large-scale data analysis, systems engineering, and program acquisition;

(U) DoD Directive 5205.16, "The DoD Insider Threat Program," outlines the roles and responsibilities for the Department's overarching program. The Department is drafting a DoD Instruction which will further implement policy, assign responsibilities, and prescribe procedures for the DITMAC.

(6) how the senior agency official, in developing the integrated, automation-assisted insider threat capability, will be supported by (A) the Under Secretary of Defense for Acquisition, Technology, and Logistics; (B) the Chief Information Officer of the Department of Defense; and (C) the Under Secretary of Defense for Personnel and Readiness; and (7) who will be responsible and accountable for managing the development and fielding of the automation-assisted insider threat capability.

(U//FOUO) In DoD Directive 5205.16, the Deputy Secretary of Defense specified the tasks and responsibilities DoD Components must perform in support of the DoD Insider Threat Program. The Under Secretary of Defense for Acquisition, Technology, and Logistics, the Chief Information Officer of the Department of Defense, and the Under Secretary of Defense for Personnel and Readiness were specifically named and assigned unique responsibilities to support the implementation and maintenance of the DoD Insider Threat Program. On December 12, 2014, the Under Secretary of Defense for Intelligence directed the Defense Security Service to establish the DITMAC. The DITMAC will leverage a wide spectrum of automated data feeds to assess risk, refer recommendations for action, synchronize responses, and oversee resolution of identified issues on threats that insiders may pose to their colleagues and/or DoD missions and resources. The Department is developing both a DoD Instruction and a subsequent DoD Manual to address these issues.

(b) INCLUSION OF GAPS.-The report required under subsection (a) shall include specific gaps in policy and statute to address the requirements placed on the Department by section 907(c) of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113-66) and Executive Order 13587. (c) STRATEGY FOR MODERNIZING PERSONNEL SECURITY DEFINED.- In this section, the term "strategy for modernizing personnel security" means the strategy developed under section 907(c) of the National Defense Authorization Act for Fiscal Year 2014 (Public Law 113- 66).

(U) Section 907(c) of the National Defense Authorization Act (NDAA) for Fiscal Year 2014 (Public Law 113-66), required the Secretary of Defense, the Director of National Intelligence (DNI), and the Director of the Office of Management and Budget (OMB) to jointly develop, implement, and provide to Congress a strategy to modernize all aspects of personnel security for the Department of Defense (DoD).

(U) Concurrent with the NDAA requirement, the OMB-led Suitability and Security Processes Review recommended similar comprehensive modernization for the entire Executive Branch. Led by the Performance Accountability Council (PAC), which includes DoD, DNI, OMB and the Office of Personnel Management (OPM), the Executive Branch has embarked on the *implementation of this comprehensive modernization.*

(U//FOUO) Given the whole-of-government approach, OMB Legislative Affairs arranged joint OMB/DNI/DoD/OPM briefings to the congressional oversight committee staffs which were provided on March 13, 2015.