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

JUN 27 2012

INTELLIGENCE

Mr. John P. Fitzpatrick
Information Security Oversight Office
National Archives and Records Administration
700 Pennsylvania Avenue, NW
Washington, D.C. 20408

Dear Mr. Fitzpatrick:

In response to your letters dated January 27, 2011 and January 23, 2012, enclosed please find the Final Report for DoD's Fundamental Classification Guidance Review (FCGR). This report provides a summary of our efforts from 2011-2012 to facilitate implementation of section 1.9 of Executive Order 13526.

We appreciate having the opportunity to work with your staff on this endeavor. If you should have any questions, please contact [redacted] at [redacted] or [redacted]

Sincerely,

For Timothy A. Davis
Director of Security

Enclosure:
As stated

cc:
Principle Deputy Director of National Intelligence

FINAL REPORT: DEPARTMENT OF DEFENSE FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEW (FCGR)

I. Introduction/Purpose.

In accordance with Executive Order 13526, *Classified National Security Information*; 32 Code of Federal Regulation (CFR) Part 2001, *Classified National Security Information*; and Information Security Oversight Office letters dated January 27, 2011 and January 23, 2012, agencies are required to complete an initial FCGR by June 27, 2012. This document provides DoD's final status report of our FCGR activities from 2011-2012 and results achieved to date.

Since our February 16, 2012 interim status report, the Department has completed the initial FCGR and is maintaining steady progress on updating our Security Classification Guides (SCG)s. Throughout this project we have focused on ensuring that classification guidance reflects current operational / warfighter needs and technical information protection requirements, while delivering up-to-date and readily available guidance on the proper classification of information. Major strides have been made in centralization of our SCGs and simplifying their dissemination and availability.

As a result of these efforts, 97% of DoD's SCGs have been updated and/or declared current, and approximately 20% of DoD's non-compartmented SCGs have either been eliminated or identified for retirement. Detailed metrics are presented in Section II, below.

II. FCGR Status Report.

a) *DoD Collateral-level (non-compartmented) FCGR Results:*

Effective June 26, 2012, DoD Components have reported the following FCGR metrics:

- Total number of SCGs identified/reported: 2,070 (up from 1,799)
- Total number of SCGs for which a FCGR has been initiated: 2,070 (up from 1,703)
- Total number of SCGs for which a FCGR has not been initiated: 0
- Total number of SCGs for which a FCGR has been completed: 2,064
- Total number of SCGs scheduled for retirement/cancellation: 413
- Total number of SCGs reported active/current: 1,657

Component-by-Component FCGR reporting details are presented at Attachment 1.

b) *Remaining Challenges*:

- Nothing significant to report.
    - Our FCGR program continues to evolve, and will remain a high-interest item for continuous attention by the Defense Information Security Advisory Board (DISAB) and the Defense Security Enterprise Advisory Group (DSEAG).
    - FCGR execution and monitoring efforts of the OUSD(I) staff are in complete alignment with DoD IG's ongoing implementation of the Reducing Overclassification Act (ROA, PL . 111-258), and we look forward to integrating results of DoD IG's ROA findings, particularly as they relate to SCG accuracy, availability, and utilization by DoD personnel.

c) *Other Initiatives:*

- OUSD(I) staff continues to generate broad FCGR lessons learned communications, as well as conduct nearly continuous Component-level engagements to improve existing SCGs, help organize the staffing process for any new SCGs, and recommend methodologies to either cancel or combine existing SCGs to create "capstone"-level SCGs. Over the past two years, this approach has resulted in the cancellation of more than 400 SCGs, nearly one-fifth of the DoD's holdings.
- In support of recent horizontal protection initiatives regarding DoD Critical Program Information (CPI), the Navy's Security Classification Guide Management Systems (SCGMS) was opened to the Acquisition Security Database (ASDB). Originally developed by Navy, the ASDB is now under the control, oversight, and management of the Director, Defense Research and Engineering (RDA) and has been designated as the DoD's central horizontal protection database. USD(I) participates in working groups and will continue to work closely with the acquisition community to achieve unity of efforts between Security and Acquisition Communities.
- Our update to DoD 5200.1H, *Handbook for Writing Security Classification Guides,* is in processing for formal coordination for conversion to a DoD Manual. We anticipate

releasing a final draft to the Components for formal review and coordination during 4Q, FY12, and signature by USD(I) in early FY13.

d) ***DoD Intelligence Community Element Reporting*:**

- Throughout the FCGR, OUSD(I) staff maintained close coordination with the ODNI/Principle Deputy Director of National Intelligence staff. Per the ODNI's previous guidance to the Intelligence Community, DIA, NGA, NSA, and NRO reported their FCGR execution status directly to ISOO, with a copy provided to USD(I).
- All DoD Intelligence Community (IC) elements successfully completed the FCGR.

e) ***Military Department FCGR Activities and Initiatives:***

- Department of the Army:
    - For many years, Army has worked to both minimize the number of its OCAs and SCGs. As a result of FCGR program developments, user community requirements, and general Service needs, the Army has established a database that contains all of the Army's collateral-level SCGs, and which is available to both security professionals and foreign disclosure officers throughout the Army. This effort parallels Army's work with DTIC to ensure their holdings are complete and maintained in an up-to-date manner.
    - Additionally, Army security professionals have met with the Army Inspector General (IG) staff on the general subject of SCGs (creation, maintenance, usage) and will assist them in developing/refining the checklists used by IG teams as they conduct security inspections. As a result, FCGR requirements and program efficacy will be routinely assessed. The Army plans to update their policies as required to ensure MACOMs also maintain a listing of SCGs that fall under their purview. There is no such requirement at present, a fact that has added to the time needed to accomplish the FCGR. As with other DoD Components, Army anticipates this effort will be ongoing long after completion of this initial FCGR; therefore reported numbers of SCGs are expected to fluctuate for some time.

- Department of the Navy:
    - The Department of Navy (DON) began with, and still maintains, the largest collection of SCGs in the DoD. The Service necessarily utilized a wide-ranging series of working groups comprised of subject matter experts, technical warrant holders, SCG users, and security professionals to complete the FCGR effort. As a current initiative, DON has identified and initiated a Security Classification Guide Management Systems (SCGMS) to effectively manage its SCGs. The SCGMS architecture and structure provides a horizontal comparison across "like" SCGs, identifying classification differences and establishing a classification baseline for information elements. Additionally, the SCGMS will be used to initiate, process, and deliver standardized SCGs via common templates; track SCG compliance across the DON commands and warfare functional areas; and provide SCG graphic visual aids (graphs and charts) which display key performance indicators. The SCGMS will support a metrics-based management and trend analysis capability for assessing overall compliance and process efficiencies such as SCG turnaround time, repetitive cycle time, and resource utilization in managing the SCG program, all key inputs necessary to inform leadership on program efficiency and effectiveness.

- Department of the Air Force:
    - The Air Force pursued an aggressive, dual-pronged approach to FCGR execution: the Original Classification Authority (OCA) population and the universe of SCGs were reviewed against EO 13526 requirements, in order to determine and validate requirements for OCA positions and to identify and cancel duplicative SCGs. As a result, the Air Force achieved a 29% decrease in OCAs thru the period of this report. The service will likely continue to identify OCA positions for whom a demonstrable and continuing need for that authority is lacking, and eliminate them.
    - Developing and validating the Air Force's inventory of SCGs was extremely challenging yet productive. The large drop-off achieved in Air Force SCGs was

due to entries for many old and/or obsolete SCGs which were improperly categorized on the legacy master list. During FCGR execution, the Air Force separated these kinds of documentation updates from its work actually conducting the FCGR, and therefore did not certify that all updates have been provided to DTIC with the applicable DD Form 2024, *DoD Security Classification Guide Data Elements."* The Air Force is, however, well postured to formally manage this follow-on phase as FCGR work will continue.

- The Air Force managed the FCGR process primarily through collection of a series of monthly and weekly suspense reports, designed to keep OCAs and security professionals sharply focused on the task. The primary lesson learned was the difficulty in changing Service SCG methodology, from a long history of improperly managing many SCGs at the unit, wing, MAJCOM, and Air Staff levels.
- As of this report, the Air Force has zero overdue SCGs, and all MAJCOMs with SCGs are acutely aware of the requirement to properly manage SCGs. The Air Force will continue with its oversight of this project at all levels to ensure that SCG creation, management, and retirement is routine and well managed.

f) *Joint Staff*

- As of June 25, 2012, all Joint Staff SCGs are deemed compliant with current security classification policy and have been evaluated as part of the FCGR. The Joint Staff and the Combatant Commands conducted the FCGR via formal tasking utilizing the Joint Staff Action Process (JSAP), in order to identify the SCGs under their purview and conduct a quality review.
- Methodology: The JS's FCGR review relied upon subject matter experts both internal and external to the organization bearing primary equity for the information, while addressing the following elements:
    i. Evaluation of overall SCG content;
    ii. Determination that the information conforms to the current operational and technical circumstances and user community requirements;

iii. Ensuring the SCG meets the classification standards and criteria under section 1.4 of the Order, and damage assessments meet criteria under section 1.2 of the Order;

iv. Dissemination and availability of the guidance is to the proper users, and is appropriate and timely;

v. Considers a review of decisions based on the guidance to ensure they reflect the intent of the guidance as to what is classified, the level of classification is appropriate, and the information is properly marked for duration and declassification;

vi. None of the Combatant Commands indicated that any JS equity information had been declassified because of the FCGR, therefore no summaries will be released to the public.

- Challenges: Obtaining Combatant Commands' focus to collect information necessary to complete this type of data call in the midst of engaging in on-going military operations and missions.
- Summary: The Joint Staff Security Office will continue to provide oversight at all levels to ensure all SCGs are properly created, managed, maintained, and routinely reviewed for currency. The primary methodology to do this will be via an annual data call to collect necessary information and ensure ongoing oversight of the SCG review process.

g) ***Defense Agencies***

- Defense Information Systems Agency (DISA):
    - Like all Components, DISA was extremely active in its FCGR process execution. Agency leadership continues to work with its subject matter experts to determine the way-forward for several SCGs for which a final resolution and way-forward decision is pending. USD(I) will continue to closely monitor the Agency's progress and projects final compliance and project completion by August 31, 2012.

- Defense Advanced Research Projects Agency (DARPA):

- DARPA maintains a small number of highly technical SCGs. A brief summary of primary topics of information classified by DARPA OCAs include: Cyber Defense, Manned Platforms, Space Operations, and Electronic Warfare. As a result of the FCGR, all of DARPA's SCGs were successfully inventoried, assessed, and deemed compliant with extant security classification policy. Necessary updates were provided to DTIC with the applicable DD Form 2024. Ultimately, no broad categories or families of classified information were declassified as a result of the DARPA FCGR effort.
- To ensure successful FCGR execution, DARPA formed internal working groups and dispatched SCGs to the appropriate DARPA technical office subject matter experts who examined all classification decisions and the SCG's relevancy. Recommendations were provided to the applicable OCAs for final determination as to the guide's status.

- Defense Threat Reduction Agency (DTRA):
  - DTRA classifies information that deals with but is not limited to the research and development of capabilities to reduce, eliminate, and counter the threat of, and mitigate the effects of Weapons of Mass Destruction (chemical, biological, radiological, nuclear) and high-yield explosives. Because of this sensitive, current, and ongoing mission, all of the information contained in cancelled DTRA SCGs was deemed to be properly classified in current SCGs, and none was declassified.
  - To ensure that classification guidance is relevant to current circumstances, DTRA assembled a working Group consisting of information security, program managers (PM), topical subject matter experts (SME) and enterprise security managers (SM). PMs and SMEs reviewed the SCGs for completeness, applicability and clarity. Enterprise SMs and information security personnel reviewed each guide for compliance with current security classification policy.
  - As of June 26, 2012, all DTRA SCGs are deemed compliant with current security classification policy and have been evaluated as part of the FCGR. A final copy

of all SCG updates (along with the DD Form 2024). will be provided to DTIC no later than September 30, 2012.

- Lessons Learned: Agency PMs and senior leadership must be alert to and educated early on regarding the importance of establishing and integrating the results of an SCG WG from the onset of a new program or revision to an existing program. The close interaction of SMEs, PMs and SMs is a vital contributor to ensure proper classification of program information. In conjunction with the SCG WG, information security personnel must implement a tracking system for each SCG, per classified and/or technical program. This tracking system is vital due to the turnover rate of personnel who are tasked with the initial writing and maintenance of published SCGs. The tracking system should also ensure proper advance notification of the SCG's five year review requirement. This tracking system should also track the distribution of the SCG and DD Form 2024, and deployment is expected during FY13.

- Missile Defense Agency:
  - MDA is a highly technical agency executing a complex mission that requires a robust and effective information security program and protection environment.
  - As a result of the FCGR, MDA certified that each SCG and the Agency declassification guide was updated IAW E.O. 13526. All SCGs have been provided to Defense Technical Information Center (DTIC) with the applicable DD Form 2024.
  - Overall FCGR approach:
    - MDA has a standing procedure for a Classification Policy Panel (CPP) composed of technical subject matter experts from across MDA to review every SCG developed or updated by the Agency (not including administrative updates), to ensure proposed topics of classification are technically accurate and relevant to the mission. The CPP is chaired by the Agency's Director for Engineering (MDA/DE) and administered by the Research, Development, and Acquisition Security Division (MDA/DEW). DEW works with the CPP technical representatives and

other subject matter experts throughout the Agency to ensure proposed topics of classification are consistent and compliant with E.O. 13526 requirements.

- Each MDA SCG not already undergoing update during the time the FCRG was initiated was reviewed by a 4-person team of classification management security specialists. The reviews validated compliance with current security classification policy (i.e., E.O. 13526) and administrative requirements; as required, SCGs were updated. Technical subject matter experts were consulted, as needed, to review SCG topics of classification to verify topic relevance.
- MDA's best practices and FCGR lessons learned:
- Best practices:
    - The 4-person review process enabled a thorough review and allowed for additional opportunities to note and correct discrepancies.
    - Achieving early compliance with DoD policy (DoD Manual 5200.01, "DoD Information Security Program,") enables the Agency to validate the relevance of SCGs and ensure continued compliance with updated policy requirements.
    - All MDA SCGs are reviewed by the agency's CPP as they undergo development or when updated. The CPP is made up of technical experts from each of the agency's programs who ensure the classification topics used in the SCGs are relevant and properly applied from a technical perspective.
    - Security (MDA/DEW) administrative support to the CPP ensures that horizontal protection of program information remains an area of emphasis.
- Lessons learned: Maintaining standardized formatting for all Agency SCGs helped to expedite traditional reviews and ensures SCGs are more consistent when used by Agency personnel. It also simplifies broader

reviews (such as those required by the FCGR) because administrative language can be more easily identified and edited, as necessary.

h) ***Training and Education Product Developments*:**

In support of the Department's execution of the FCGR, the Center for Development of Security Excellence (CDSE) has completed a Derivative Classifier's course, available from the CDSE and Security Directorate website. The CDSE team has also completed an OCA "short" course, intended to cover all training requirements for OCAs required by EO 13526 and DoD regulations.

i) ***Migration of Legacy Classification Guidance from DoD Issuances*:**

The DoD's FCGR has revealed the existence of potentially duplicative or obsolete classification management guidance or SGCs embedded within or provided thru DoD issuances (instructions, directives, regulations, etc.). DoD's Information Security Program (DoD Manual 5200.01, Volume 1) requires that all non-ACCM, SAP, SCI, or extraordinarily sensitive SCGs are to be distributed to DTIC, ultimately for posting to its website on NIPRNet and/or off-line availability to SIPRNet users. We will continue our effort to review all issuances to compare SCGs promulgated as DoD issuances, with those in the DTIC's holdings. To date, we have identified eighteen such SGCs that are not yet reflected on DTIC's website. This project is ongoing, and may also result in new SCGs being developed (under/through the OCA-to-DTIC process); further cancellation of obsolete guidance on the issuances website; or merging of content between the two, in order to deliver an updated product to DTIC.

j) ***Unresolved/Open Issues:***

- An amendment to this report will be forthcoming.
    - The DoD Special Access Program (SAP) community completed the FCGR in accordance with the requirements of the USD(I)'s tasking. However, the formal response memorandum is pending signature and will be forwarded by early July, 2012.
    - The Office of the Under Secretary of Defense for Policy (OUSD(P)) completed the FCGR. Although OUSD(P) renders original classification decisions on a

number of international policy issues, the Office concluded, as a result of the FCGR, that they do not have a satisfactory level of foundational security classification guidance in place, and have initiated development of a condensed set of broad and overarching SCGs to provide that guidance. This project is extremely complex, requires adjudication of multiple cross-OCA equity issues, and the results will be reported as an amendment to this report as soon as possible. Three extant SCGs within OUSD(P)'s claimancy are reflected in the OSD Element count (see Attachment 1, below); however, this number will be adjusted depending upon OUSD(P)'s ongoing reassessment.

DOD COMPONENT-BY-COMPONENT FINAL REPORT
FUNDAMENTAL CLASSIFICATION GUIDANCE REVIEW[1]

Organization	Total Number of SCGs	FCGRs Initiated	FCGRs not initiated	FCGR Completed	SCGs Eliminated	Active SCGs	Remarks
Air Force	306	306	0	306	44	262	
Army	417	417	0	417	72	345	
DARPA	159	159	0	159	25	134	
DCMA	1	1	0	1	0	1	
DISA	7	7	0	1 (see remarks)	1	6	• Initial review completed. • Working with SMEs/ OCAs on way-forward for remaining SCGs. • ECD: August 31, 2012.
DLA (new guide)	1	1	0	1	0	1	
DTRA	55	55	0	55	13	42	
JIEDDO	1	1	0	1	0	1	
Joint Staff (includes COCOMs)	95	95	0	95	9	86	
MDA	29	29	0	29	0	29	
Navy	988 (820)	988	0	988	248	740	
OSD Elements	11	11	0	11	1	11	• See paragraph (j), above, regarding OUSD(P) initiatives. • One USD(I) Guide to be transferred to Joint Staff & potentially eliminated.
DoD Totals	**2070 (1799)[2]**	**2070**	**0**	**2064**	**413**	**1657**	

ATTACHMENT 1

[1] This report does **not** reflect NGA, NRO, NSA & DIA FCGR metrics and reporting. These Components reported directly to ISOO, cc: to ODNI and OUSD(I).
[2] Reflects an updated total SCG count from the DoD's 3rd Interim FCGR Report (February 16, 2012)