Volume XV, Issue 1

February 2004

INFORMATION CLASSIFICATION AND CONTROL POLICY (ICCP)

CommuniQué

From the Director's Office:

Much has changed since our last issue of the CommuniQué. The most recent and perhaps the most surprising change was Secretary Abraham's announcement that the Department of Energy (DOE) has established the new Office of Security and Safety Performance Assurance (SSA). This action followed a comprehensive review by Deputy Secretary Kyle McSlarrow that identified the need to reform and better coordinate the roles of independent oversight and the security policy organizations within DOE. This new organization should strengthen our national security by ensuring that DOE's security policies and procedures are implemented correctly.

The two major branches of the new office, the Office of Independent Oversight and Performance Assurance (OA) and the Office of Security (SO), will remain independent of each other. Mr. Glenn Podonsky, the former head of OA, is the Director of SSA and reports directly to the Secretary. Mr. Marshall Combs has been designated as the Director of SO, and Mr. Michael Kilpatrick has been designated as the Director of OA. Both were former Deputy Directors of their respective Offices.

A review of SO and OA is being conducted and changes to increase the efficiency of both organizations are planned. In its evaluation, SSA is taking a "back to the future" approach to identify what worked best in the past and applying it to the future. Although it is too early to discuss specifics, we expect some traditional organizations and relationships to be reestablished. The reorganization should be announced in the late March time frame.

Another significant change is the issuance of a major revision to Executive Order (E.O.) 12958, *Classified National Security Information*. Although it is not a complete rewrite, there are significant changes that will affect the way we do business. An article in this newsletter highlights these changes. Needless to say, my staff is working diligently to update appropriate directives and guidance to reflect the new requirements. This will be a lengthy process so your patience and input will be appreciated.

Another major milestone was the publication of the Official Use Only (OUO) order, manual, and guide. These products represent years of work and give us a legal basis for protecting unclassified information in a variety of subject areas. Hopefully, over time, these directives will reduce the existing proliferation of ad hoc control measures for various kinds of unclassified information that have appeared throughout DOE. When appropriate, classification guides

Director *(Continued on page 4)*

Changes to Executive Order 12958 "Classified National Security Information"

On March 25, 2003, President Bush signed an amendment to E.O. 12958. The amendment is the result of almost 2 years of diligent effort by interagency working groups composed of representatives from the Government-wide classification community. Although the primary impetus for the amendment was to address the impending deadline for automatic declassification (April 17, 2003), agencies also discussed a number of classification issues and concerns that have surfaced in the past few years. The amendment, with its extensive revisions, addresses many of these issues.

Here are some highlights:

- The deadline for automatic declassification of classified records more than 25 years old in collections determined to have permanent historical value has been extended from April 17, 2003, to December 31, 2006.
- The "significant doubt" provision for origi-

E.O. 12958 *(Continued on page 2)*

Inside this issue:

Special points of interest:

- *Derivative Classifiers — What goes on the "Declassify On" line? — See "Revised Declassification Instructions" on Page 2.*
- *What's new on Identifying and Protecting Official Use Only Information? — See Page 4.*
- *What classification/UCNI guides are being developed/revised — See Page 5.*

E.O. 12958 *(Continued from page 1)*

nal classification has been deleted. Similarly, the "significant doubt" provision for level of classification has also been deleted.

- The presumption of damage for the unauthorized disclosure of foreign government information has been put back in the E.O.
- "Weapons of mass destruction" has been added as a classification category.
- Normal duration of classification has been extended from 10 to 25 years. As a result, the exemption from declassification at 10 years has been eliminated, and the use of 10-year exemption categories (X1-X8) will be discontinued. This change still allows for records to be declassified at 10 years, but also equally allows for declassification to be specified at any duration up to 25 years.
- Information may be reclassified after declassification and release to the public under strict conditions.
- In emergency situations, the agency head or any designee may authorize the disclosure of classified information to an individual or individuals who are otherwise not eligible for access.
- The concept of documents being filed in an "integral file block" is introduced, allowing agencies to process records subject to automatic declassification using standard records management procedures.

ICCP is beginning the process of implementing the E.O. changes through its directives and classification guides. If you have any questions on this amendment to the E.O., please contact ICCP at (301) 903‑9048.

Emily Puhl, Policy and Quality Management (PQM), ICCP

Revised Declassification Instructions for National Security Information (NSI) Documents

The amendment of E.O. 12958 and the issuance of its implementing directive by the Information Security Oversight Office (ISOO) have sparked a flurry of activity for Technical Guidance staff. NSI topics in Headquarters (HQ) classification guides need to be evaluated and page changes issued over the next several months to bring the guides into conformance with the revised E.O. requirements. Once those page changes are issued, COs will also need to update their local guides. In the interim, Derivative Classifiers (DCs) should continue to apply the markings as indicated in current guidance. For example, if a topic states information is "SNSI[X1]," then the DC should put "X1" on the "Declassify On" line of the DC stamp. If the topic gives a date or event, the date or event should be placed on the "Declassify On" line.

One of the biggest changes that the revised guides address is the end of automatic declassification at 10 years. The guide topics will now include one of the following three kinds of declassification instructions: a specific date up to 25 years from the date the information was classified (e.g., July 1, 2008), a duration in years to be added to the date of the document to determine the date for declassification (e.g., [25]), or a specified event that should occur within 25 years that must be detailed in the text of the topic (e.g., when a vulnerability no longer exists). When the declassification instruction is a duration in years, the DC must convert this to a date. For example, if the guide topic used to classify a document that was generated on January 3, 2004, showed a duration of [25], the DC would annotate the stamp, "Declassify On: January 3, 2029."

Another major change will allow a DC to classify a document for longer than 25 years. This is possible if the classification guide topic covers information that has been exempted from declassification at 25 years in an ISOO-approved declassification guide (i.e., Historical Records Declassification Guide, CG-HR-2). The classification guide topic will include the designation "[25Xn]" following the classification designation, where the "n" refers to the appropriate number of the exemption category in E.O. 12958, section 3.3(b)(1)-(9). The topic must also include declassification instructions such as a specific date, a number of years to be added to the date of the document to determine the date for declassification, or a specified event (must be detailed in the text of the topic). If the exemption pertains to the identity of a confidential human or human intelligence source, such information is never automatically declassified and is marked as "25X1, human." A DC must put the 25Xn and the declassification date or event on the "Declassify On" line of the stamp. For example, if the guide topic used to classify a document that was generated on January 3, 2004, showed a duration of [25X1, 40], the DC would annotate the stamp, "Declassify On: 25X1, January 3, 2044."

DCs should consult the *Index of Headquarters Classification Guidance* to make sure they have the most current changes to their guides. If you have any questions concerning this policy, contact ICCP at (301) 903-5454.

Linda Brightwell, PQM, ICCP

Administrative Note

Although the primary means of distributing the CommuniQué will be electronically, a limited number of hard copies are available. You may request hard copies by contacting Pat Rhoderick at (301) 903-3637 or by e-mail at pat.rhoderick@hq.doe.gov. You may also make changes to our distribution list through Pat.

Outreach Corner

The ICCP PQM staff continues to conduct Quality Assurance Reviews (QARs) in accordance with Public Laws 105-261 and 106-65, sections 3161 and 3149. Since the last CommuniQué, PQM has visited the Washington Headquarters Service (WHS), the Air Force Technical Applications Center (AFTAC), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA). WHS and AFTAC met all of the requirements of the Special Historical Records Review Plan (Supplement) (the Plan). The FBI and NSA were lacking implementation plans required by the Plan but have developed draft plans since the QAR.

The Public Laws requiring agencies to protect against the inadvertent release of Restricted Data (RD) and Formerly Restricted Data (FRD) have been around for a little over 5 years, and recent QARs indicate that agencies, for the most part, are complying with the Plan and preventing the inadvertent release of RD and FRD. Although PQM will continue to conduct QARs and monitor the declassification programs of previously visited agencies, this seems like the right time to shift the focus of visits to those organizations that currently have access to RD and FRD information and generate and control RD and FRD documents. Initially, this will be in the form of visits to agencies' RD Management Officials, but eventually we hope to conduct onsite visits to evaluate how well agencies and organizations are implementing 10 Code of Federal Regulations Part 1045, *Nuclear Classification and Declassification*.

These visits will be discussed at an RD Management Officials Meeting that will be held sometime this spring. The agenda for the meeting is currently being developed. In the meantime, any agency/organization that would like an onsite visit by PQM to provide feedback on its RD classification program should contact the DOE Outreach Hotline at (301) 903-7567. After the visit, PQM will provide the agency with a report and any assistance that may be needed.

Other services PQM provides include reviewing RD training material, assisting agencies in developing RD training material, and providing existing training materials, such as the computer-based training disk entitled Restricted Data Classifiers Course. If you have any questions concerning the ICCP Outreach Program and the services that it can provide, contact Rita Metro, (301) 903-1152 or rita.metro@hq.doe.gov.

Electronic Classification Guidance System (eCGS)

A major part of the Guidance Streamlining Initiative is modernizing the Classification Guidance System. ICCP took its first step in this process when it issued the new eCGS, Version 03.1, in June 2003. It contained all classification guidance received and approved prior to April 15, 2003.

This new eCGS version maintains the classification guides in the Portable Document Format (PDF) that allows published guides to be presented in a format closely matching their paper version. More importantly, this new system is more easily maintained and allows existing support staff to hasten the migration of all guidance data to eXtensible Markup Language (XML). Once classification guidance is in XML format, ICCP can manage, organize, and edit classification topics more effectively and provide more powerful search capabilities and knowledge-based tools to the classification community.

While there are subtle differences in the search techniques between the old and new systems, eCGS has full-text search functions equivalent to the previous CGS. A User's Guide, which includes instructions for installing the application onto a hard drive of a classified computer system for optimum speed, is available on the eCGS compact disk. Until all classification guides are converted to XML, eCGS based on the PDF format should provide adequate search capabilities.

To facilitate rapid production of future eCGS versions, local guides should be submitted for approval in the text-PDF format. This PDF can be generated from the original electronic word processor file or can be sent using acrobat distiller. eCGS will be updated semi-annually in January and July, and the production cut-off dates for updated versions are December 31 and June 30, respectively.

To obtain a copy of eCGS, submit a request through your CO to the Director, Technical Guidance, ICCP. Your CO should have the required forms. For further information concerning eGCS or XML, contact ICCP at (301) 903-4648. Suggestions on ways to improve the system are always appreciated.

Vinh Le, TGD, ICCP

Upcoming Events

March 23—Classifiers Course, HQ
March 23-25—Oversight Review, Portsmouth Gaseous Diffusion Plant
March 30-April 1—Oversight Review, Paducah Gaseous Diffusion Plant
March 30-31—Derivative Declassifiers Course, Albuquerque, NM
April 10—QAR of the National Aeronautics and Space Administration (NASA), Washington, D.C.
April 19-22—Historical Records Restricted Data Reviewers Course, HQ
May 11-13—Classification Officers Meeting, HQ
June 8—Classifiers Course, HQ
June 8-11—Oversight Review, Oak Ridge Operations Office
July 20-21—Derivative Declassifiers Course, HQ
July 26-30—Overview of Weapons Classification Course, HQ

Director *(Continued from page 1)*

will incorporate topics to help identify OUO information. An article in this newsletter summarizes the contents of these publications and highlights their requirements.

On May 13, 2003, I had the pleasure of presenting the 2003 Classification Award of Excellence to Mr. Rick Stutheit, Classification Officer (CO), Richland Operations Office, and Mr. Dave Briggs, Manager, National Security Analysis Team, for their dedicated work on the Hanford Declassification Project. As a result of their efforts, numerous historical Hanford Site documents were released to interested parties without sacrificing our national security. Again, congratulations on a job well done. This year's Classification Officers Meeting is rapidly approaching (May 11-13). Don't forget to submit your nominations for the 2004 Award of Excellence.

Finally, we have used the time since the last CommuniQué to make a few changes. In addition to the new format, the primary means of distribution is now via e-mail. This will not only allow us to use multiple colors but also gives us the flexibility of expanding it to as many pages as necessary to ensure complete coverage of all relevant material. We will continue to make improvements and encourage you to make recommendations for articles or submit your own.

Joan G. Hawthorne, Director, ICCP

REMINDERS

- Derivative classifiers do not have the authority to declassify or downgrade information or documents.
- Only Federal personnel can be granted original classification authority.
- All original classification determinations must be reported to ICCP with 10 working days of the determination.
- Confirmation, denial, or expansion upon public statements covering classified information is prohibited.

Moments in History

Governments aren't the only organizations that have protected information throughout history. In the 17th century in the du Pain part of France, bakers protected Secret bread recipes. Access to the recipes was on a strict "knead-to-know."

The U.S. Constitution (1787) approved secrecy in Article I, Section 5, when it authorized the House of Representatives and Senate to publish a journal of their proceedings, "excepting such Parts as may in their Judgment require Secrecy."

This is Your Newsletter

The CommuniQué will be published quarterly. Remember that this publication is for the classification community as a whole and we welcome input. If you are interested in submitting an article or suggesting a subject area to be covered in an article, please contact Nick Prospero at (301) 903-9967 or by e-mail at nick.prospero@hq.doe.gov.

Identifying and Protecting Official Use Only Information

On April 9, 2003, DOE issued directives that formally establish an OUO program within DOE for the first time since the Atomic Energy Commission. The OUO directives package consists of:

- DOE Order 471.3, *Identifying and Protecting Official Use Only Information,* which contains requirements and responsibilities;
- DOE Manual 471.3-1, *Manual for Identifying and Protecting Official Use Only Information,* which provides instructions for implementing requirements; and
- DOE Guide 471.3-1, *Guide to Identifying Official Use Only Information*, which provides information to assist someone in deciding whether information could be OUO.

These directives apply to all DOE and National Nuclear Security Administration (NNSA) elements that (1) identify information under their cognizance as OUO and mark documents accordingly or (2) possess documents marked as OUO by other DOE elements or marked with other-agency markings equivalent to OUO (e.g., Department of Defense's (DoD) "For Official Use Only"; Department of State's "Sensitive But Unclassified").

Although issuance of these OUO directives is a quantum leap forward in DOE's effort to identify and protect only that unclassified information that can be legally controlled, it is only a start. To be effective, the requirements of the program must be understood and implemented throughout DOE and NNSA. While COs do not have any specific responsibilities identified in the directives, they are considered information security experts and, therefore, may play a central role in implementing the OUO program at their sites and offices. Becoming familiar with what is required by these directives is essential, and the following questions and answers should help with that task. Any questions concerning the OUO directives should be addressed to ICCP staff at (301) 903-5454.

Who can determine if a document contains OUO?

Any employee, Federal or contactor, can determine that an unclassified document contains OUO information if that document is originated within his/her office, is produced for his/her office, or is under the control of his/her office. No special authority or training is required. However, the employee should be familiar with (1) the requirements and in-

OUO *(Continued on page 6)*

Guidance Status

Classification Guides (CG)

CG-CM-1. New CG concerning activities of the gaseous diffusion membrane technology transfer under the Commercial Membrane Corporate Research and Development Agreement has been developed. Approval is expected in early 2004.

CG-DNC-2. Revision to the CG for codewords, designators, and nicknames is in the final stages of development. Draft of the revision was distributed to the field for comment on June 4, 2003. After all the comments have been addressed, the guide will be formally coordinated.

CG-ECIS-1. New CG for energy critical infrastructure information is being developed. A first draft was prepared for DOE's Office of Energy Assurance to cover the August 14, 2003, power blackout. DOE and the Department of Homeland Security (DHS) are jointly preparing the guide.

CG-EM-1. New CG for environmental monitoring is being developed. First working group meeting is in February 2004, at Patrick Air Force Base in Florida. This CG will provide guidance for the rapidly improving environmental sampling capabilities used in support of national and international arms control and nonproliferation objectives.

CG-EPW-1. Draft CG for the robust nuclear earth penetrator weapon is in the final stages of development. After comments from the DoD are received and addressed, ICCP will meet with the Air Force Strategic Command and Air Combat Command. Final coordination of the guide should begin in March 2004.

CG-HRW-1. CG on historical radiological warfare information is on hold pending declassification actions.

CG-LCP-2. Revised CG on the Louisiana Energy Service Gas Centrifuge Program has been sent to the UK for final review and approval.

CG-MTI-1. CG for the multispectral thermal imager program should be approved in February 2004. CG will provide guidance for system performance, data measurement, and data analysis. Program is used by Government sponsored researchers and academia.

CG-NMI-1. New CG for nuclear material inventories is near final development. Approval is expected in early 2004.

CG-OCRWM-1. New joint DOE/ Nuclear Regulatory Commission CG for civilian radiological waste management has been developed. Approval is expected in early 2004.

CG-PSP-1. New CG for the plasma separation process was reviewed at a working group meeting in October. Technical issues are being addressed. Approval is expected in mid-2004.

CG-PSPR-1. DOE and NASA have initiated a new guide covering the Prometheus Space Power Reactor program. A working group that includes NASA, Jet Propulsion Laboratory, Los Alamos National Laboratory, Y-12, and the DOE Nuclear Energy Office of Space and Power Systems has been formed.

CG-SCE-1. Page change to the subcritical experiments CG that incorporates revised mass limits is under development.

CG-SMG-2. Major revision to the CG for nuclear smuggling information has been completed and approved. This CG covers radiation detection at U.S. Customs and Border Protection controlled ports-of-entry to the U.S. and foreign border crossings under the DOE's Second Line of Defense program. Associated information addressed in the guide includes nuclear threat information; analysis, research, development, and radiation detection equipment testing information; operational radiation detection systems; weapons materials and design information; forensics; and incident response and reporting. This CG represents the first collaborative project for identifying sensitive information between ICCP and DHS.

CG-SS-4. Major revision of this CG is underway. Working groups have formed to address Protection Program Operations and Material Control and Accounting. The working groups will develop drafts that will be distributed to all COs and HQ Classification Representatives for review and comment.

CG-SSP-2. Revision to the CG for the stockpile stewardship program is being developed. The first working group meeting will be in February 2004, at Albuquerque, NM. The group will determine which classification topics should be eliminated, transferred to other guides, or retained in the revised CG-SSP-2.

CG-UAV-2. Revision of this CG is complete and approval is expected in the near future.

CG-UK-1. A page change to this guide is being reviewed by the UK. Approval is expected in the near future.

USEC. A working group meeting for the United States Enrichment Corporation's (USEC) gas centrifuge CG was held in January 2004 at Oak Ridge. A final draft will be prepared by USEC and submitted to ICCP for publication. Approval is expected by mid-2004.

Topical Classification Guides (TCG)

TCG-DS-1. Revision to the TCG for detonation systems is being developed. First working group meeting was held in January 2004, at Sandia National Laboratories/NM (SNL/NM). Revised CG will incorporate new technological developments and add use control information.

TCG-SAFF-2. Revision to the TCG for safing, arming, fuzing, and firing has been developed. The CG has been with the DoD since last spring for coordination. Once comments have been received and addressed, the CG will be formally coordinated.

Guidance *(Continued on page 6)*

OUO *(Continued from page 4)*

structions for implementing those requirements contained in these directives and (2) any OUO guidance that may have been issued by his/her program office or SO.

How are these OUO determinations made?

As outlined in the manual, the first step is for the employee to determine if the information has the potential to damage Governmental, commercial, or private interests if given to someone who doesn't need it to perform his/her job or other DOE-authorized activity. In some cases, the program office may already have made this determination and issued guidance that states such information is OUO. (For example, if the guidance states: "The number of guards at building X is OUO," the program office has determined that merely revealing the number of guards would meet the damage criteria.) In other cases, the employee must determine if the information meets certain criteria outlined in the guidance in order to make the determination. (For example, if the guidance stated "The number of guards at building X is OUO if an exploitable vulnerability exists," the employee must determine if there is an exploitable vulnerability before making the OUO determination.)

If no guidance exists and the employee believes that the information could damage a Government, commercial, or private interest, the employee must determine if the information falls under at least one of the Freedom of Information Act (FOIA) exemptions 2 though 9. All Government information control systems must be consistent with the FOIA exemptions since there is not much point to trying to control information if it cannot legally be protected from disclosure under the FOIA. Many employees are not familiar with these exemptions or the types of information covered by them. That is why DOE Guide 471.3-1 was developed. It contains the FOIA statutory language, a brief "plain English" description and explanation of each exemption, and some examples of the types of information that could be OUO for each exemption. If the employee believes that release of the information would cause the damage described and the information falls under one of the FOIA exemptions, then the information is OUO. This connection between OUO and the FOIA exemptions should not lead anyone to believe that just because a document is marked OUO, it is automatically FOIA exempt. Every OUO document requested under the FOIA must be reviewed from scratch under the FOIA rules since the information may have lost its sensitivity over time--or perhaps it was never really sensitive and should not have been marked OUO in the first place.

How are documents containing OUO information marked?

DOE Manual 471.3-1 provides extensive information on how to mark OUO documents (e.g., front marking, page marking, marking e-mail messages, marking special format documents, marking transmittal documents) that won't be repeated here. Some changes to take note of are that:

- the front marking now must include both the FOIA exemption number and the descriptive category name (e.g., 2 – Circumvention of Statute);
- the page marking is only required at the bottom of each page as opposed to top and bottom; and
- if guidance was used to make the determination, the front marking includes a line to identify the guide that was used (e.g., CG-SS-4). [NOTE: If the OUO determination is not based on guidance but on a person's decision that the information is sensitive and falls under one of the FOIA exemptions (as described in DOE Guide 471.3-1), then this line should be left blank.]

Who can have access to an OUO document?

Any person (to include local government officials and foreign nationals) who requires the information to perform his/her job or other DOE-authorized activities may have access to an OUO document. Such access is granted by the person in possession of the document.

How is an OUO document protected?

Reasonable precautions should be taken to preclude access to the information by those who don't need it for official activities.

- If after-hours building security is provided, the document may be stored in an unlocked receptacle, such as a file cabinet, desk, or bookcase.
- If such security is not provided, then the document must be stored in a locked receptacle.
- OUO documents may be reproduced to the minimum extent necessary, ensuring that all copies are marked as required.
- OUO documents may be destroyed by using a strip cut shredder that produces strips no more than ¼ inch wide or by any other locally approved method.
- When sending an OUO document by mail, place it in a sealed, opaque envelope and write "To Be Opened by Addressee Only" on the outside.
- When transmitting OUO information by fax or e-mail, use encryption methods approved for unclassified controlled information (e.g., Entrust) whenever possible. If encryption is not available and mailing is not a feasible alternative, then regular fax or e-mail may be used.
- To process OUO information on a computer, the system must prevent access by unauthorized persons (e.g., use of password or file access controls).

Complete details on protection and processing requirements are contained in DOE Manual 471.3-1.

Linda Brightwell, PQM, ICCP

Guidance *(Continued from page 5)*

TCG-WM-2. Revision to the TCG for weapon materials is being developed and a working group meeting was held in February 2004, at SNL/NM. Comments from the working group will be incorporated into the draft CG and distributed to the field for comment.

TCG-WPMU-2. Revision to the TCG for weapons production and military use has been developed. The CG has been in coordination with the DoD for the last 2 years. The latest set of DoD comments has been received and incorporated. The guide is in final coordination and will be submitted to DoD for signature in the near future.

Topical Guidelines (TG)

TG-NNP-2. Revision to the nuclear nonproliferation TG is in process.

Andy Weston-Dawkes
Director, Technical Guidance