

This document is made available through the declassification efforts
and research of John Greenewald, Jr., creator of:

The Black Vault



The Black Vault is the largest online Freedom of Information Act (FOIA)
document clearinghouse in the world. The research efforts here are
responsible for the declassification of hundreds of thousands of pages
released by the U.S. Government & Military.

Discover the Truth at: <http://www.theblackvault.com>

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, DC 20511

JAN 29 2016

John Greenwald, Jr.
[REDACTED]
[REDACTED]

Reference: ODNI Case DF-2016-00127

Dear Mr. Greenwald:

This responds to your FOIA request of 28 January 2016 (Enclosure 1), received in the Office of the Director of National Intelligence (ODNI). You requested a copy of ICD 701, Security Policy Directive for Unauthorized Disclosures of Classified Information.

A search of our records and databases located the document you requested, "ICD 701, Security Policy Directive for Unauthorized Disclosures of Classified Information". This document was previously released under FOIA case DF-2010-00112. A copy of the document is provided at Enclosure 2.

If you have any questions, feel free to email our Requester Service Center at DNI-FOIA@dni.gov or call us at (703) 874-8500.

Sincerely,

Sally Nicholson
bor Jennifer Hudson
Director, Information Management Division

Enclosures

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

ICD 701

INTELLIGENCE COMMUNITY DIRECTIVE

NUMBER 701



**SECURITY POLICY DIRECTIVE FOR UNAUTHORIZED DISCLOSURES OF
CLASSIFIED INFORMATION**

(EFFECTIVE: 14 MARCH 2007)

A. (U) AUTHORITY: The National Security Act of 1947, as amended; the Intelligence Reform and Terrorism Prevention Act of 2004; Executive Order (EO) 12958, as amended, Classified National Security Information; EO 12333, as amended, United States Intelligence Activities; EO 13355, Strengthened Management of the Intelligence Community (IC); and other applicable provisions of law.

B. (U) APPLICABILITY: This directive applies to the IC, as defined by the National Security Act of 1947, as amended, and other departments or agencies that may be designated by the President, or designated jointly by the Director of National Intelligence (DNI) and the head of the department or agency concerned, as an element of the IC.

C. (U) PURPOSE: Unauthorized disclosures of classified information, including media leaks, may compromise sources and methods and pose a threat to national security. This directive establishes the DNI's policy to deter, report, and investigate unauthorized disclosures and to take appropriate protective and corrective action. This IC directive (ICD) rescinds Director of Central Intelligence Directive 6/8, dated 9 December 2002. Notification to the DNI does not affect the authorities and responsibilities of Senior Officials of the Intelligence Community (SOIC) to report to the Attorney General possible violations of federal criminal laws under EO 12333, as amended.

D. ~~(U//FOUO)~~ POLICY: SOICs shall promptly report to the DNI, via the Special Security Center (SSC), actual or suspected unauthorized disclosures including media leaks of classified

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

ICD 701

information that meet the reporting criteria in paragraph E, except for disclosures that are the subject of counterespionage or counterintelligence investigations.

E. ~~(U//FOUO)~~ REPORTING CRITERIA: The DNI directs SOICs to promptly report each actual or suspected unauthorized disclosure of classified information that is likely to cause damage to national security interests. Such disclosures may include, but are not limited to:

1. ~~(U//FOUO)~~ Unauthorized disclosure to an international organization, foreign power, agent of a foreign power, or terrorist organization.
2. ~~(U//FOUO)~~ National intelligence activities or information that may be at risk of appearing in the public media, either foreign or domestic, without official authorization.
3. ~~(U//FOUO)~~ Loss or compromise of classified information that poses a risk to human life.
4. ~~(U//FOUO)~~ Loss or compromise of classified information that is indicative of systemic compromise.
5. ~~(U//FOUO)~~ Loss or compromise of classified information storage media or equipment.
6. ~~(U//FOUO)~~ Discovery of clandestine surveillance and listening devices.
7. ~~(U//FOUO)~~ Loss or compromise of classified information revealing US or a foreign intelligence partner's intelligence operations or locations, or impairing foreign relations.
8. ~~(U//FOUO)~~ Such other disclosures of classified information that could adversely affect activities related to US national security.
9. ~~(U//FOUO)~~ Loss or compromise of classified information revealing intelligence sources or methods, US intelligence requirements, capabilities and relationships with the US Government.

F. ~~(U//FOUO)~~ REPORTING GUIDELINES: SOICs shall report via the SSC:

1. ~~(U//FOUO)~~ Actual or suspected unauthorized disclosures including media leaks of classified information.
2. ~~(U//FOUO)~~ Copies of all crime reports submitted to the Department of Justice (DoJ), concurrently with such submission to DoJ, on any actual or suspected instances of unauthorized disclosures of classified information.
3. ~~(U//FOUO)~~ Updated reports as appropriate, or as directed by the DNI, of the status of any given incident. These reports shall include:

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

ICD 701

- a. ~~(U//FOUO)~~ A complete statement of the facts.
 - b. ~~(U//FOUO)~~ The scope of the disclosure.
 - c. ~~(U//FOUO)~~ Sources and methods that may be at risk.
 - d. ~~(U//FOUO)~~ The potential effect of the unauthorized disclosure on national security.
 - e. ~~(U//FOUO)~~ Corrective or mitigating actions taken by the SOICs involved.
4. ~~(U//FOUO)~~ Final disposition of all reported cases, including sanctions administered; e.g., written or verbal reprimands, suspension without pay, revocation of clearances or special access approvals, and termination of employment.

G. (U//FOUO) OTHER SOIC RESPONSIBILITIES:

1. ~~(U//FOUO)~~ Administer to all individuals approved for access to classified information and materials appropriate non-disclosure agreements that address and reinforce the requirement for the continuing protection of all categories and levels of classified information including third party information.
2. ~~(U//FOUO)~~ Formally debrief all individuals no longer requiring access to national intelligence information. Debriefing procedures shall stress the continuing obligation to protect such information; the return of all classified information the individuals may have in their possession; and sanctions and penalties that may be imposed should the individuals fail to comply.
3. ~~(U//FOUO)~~ Identify all factors determined to have contributed directly or indirectly to the compromise of classified information and ensure they are corrected. If corrective action falls outside the available resources or authorities of the responsible SOIC, that SOIC shall provide full details and recommendations to the DNI for consideration.
4. ~~(U//FOUO)~~ Ensure the workforce understands the policies and procedures embodied in this ICD to include the impact that unauthorized disclosures have on organizations' missions and national security as well as the administrative and criminal sanctions that may be imposed on those individuals found to be in violation of applicable laws or regulations.
5. ~~(U//FOUO)~~ Oversee the hiring and retention of a trustworthy workforce that is properly instructed in the appropriate classification and handling of sensitive materials and the prohibition against unauthorized release or disclosure as it applies to individuals with former as well as current access.
6. ~~(U//FOUO)~~ Educate the workforce regarding processes and procedures for promptly reporting unauthorized disclosures including media leaks.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

ICD 701

7. ~~(U//FOUO)~~ Develop, implement, and update continuing security, counterintelligence, and security awareness programs for the protection of classified information and ensure all associated practices and procedures remain current.

8. ~~(U//FOUO)~~ If determined that an actual or suspected incident involves classified information originated by or otherwise within the responsibility of another IC element, the SOIC of the affected organization shall advise the SOIC having originator authority over the information concurrently with notification to the DNI. If such an incident involves a foreign intelligence partner, only the SOIC who manages the relationship with that specific foreign partner is authorized to report the incident to that foreign partner.

H. (U//FOUO) SSC RESPONSIBILITIES: The SSC shall:

1. ~~(U//FOUO)~~ Maintain the repository for all unauthorized disclosure reports.
2. ~~(U//FOUO)~~ Coordinate with affected elements, including the Office of the DNI /Office of the General Counsel, DoJ, and appropriate law enforcement organizations to track all incidents, compile statistics, and perform relevant data analysis.
3. ~~(U//FOUO)~~ Recommend to the DNI policies, programs, and processes to strengthen IC safeguards against unauthorized disclosures.
4. ~~(U//FOUO)~~ Provide compliance oversight.

I. (U) EFFECTIVE DATE: This ICD becomes effective on the date of signature.

J. M. McConnell
Director of National Intelligence

14 MAR 07
Date

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~