National Security Classification And Exemption 1 of the Freedom of Information Act

Exemption 1 applies to matters that are…

1. specifically authorized under criteria established by an Executive order to be kept secret in the interest of **national defense** or **foreign policy**; and
2. Are in fact **properly** classified pursuant to such Executive order

Course Overview

- Executive Order 13526 & Proper Classification
- Processing a FOIA Request & Exemption 1
- Timing of Classification and Fixing Deficiencies
- Waiver of Exemption 1
- Declassification Provisions of EO 13526
- Litigation Considerations

Executive Order 13526

- The President is responsible for protecting national security and has the power to develop policies regarding classification.
- EO 13526 was signed by President Obama in 2009 and retained by Presidents Trump and Biden.

Executive Order 13526

- EO 13526 supersedes predecessor EOs in effect under prior administrations, but information properly classified while those EOs were in effect may remain properly classified (assuming they were not declassified or officially disclosed since being classified).

Proper Classification

Two-Part Test:

- The information must fall **substantively** within one of the defined categories of the Executive Order used for classification.
- All **procedural** requirements of that Executive Order must be met.

Executive Order 13526

Classification Standards

1) Classification decisions must be made by an Original Classification Authority (OCA)
   - OCAs often have subordinate Subject Matter Experts (SME's) review the records

2) Gov't must maintain control of the information
   - An unauthorized disclosure (leak) does not nullify classification

Sec. 1.1 – Classification Standards

Executive Order 13526

Classification Standards

3) Information must fall within one of the qualifying categories in Section 1.4

4) OCA must determine that release could reasonably be expected to damage national security

Sec. 1.1 – Classification Standards

Executive Order 13526

Qualifying Categories (Substantive)

What type of information may be classified?

a) military plans, weapons systems, or operations;
b) foreign government information;

Sec. 1.4 – Classification Categories

Executive Order 13526

Qualifying Categories (Substantive) cont'd

c) intelligence activities (including covert action), intelligence sources or methods, or cryptology;

d) foreign relations or foreign activities of the United States, including confidential sources;

Sec. 1.4 – Classification Categories

Executive Order 13526

Qualifying Categories (Substantive) cont'd

e) scientific technological, or economic matters relating to the national security;

f) U.S. Government programs for safeguarding nuclear materials or facilities;

Sec. 1.4 – Classification Categories

Executive Order 13526

Qualifying Categories (Substantive) cont'd

g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, or plans or protection services relating to the national security; or

h) development, production, or use of weapons of mass destruction.

Sec. 1.4 – Classification Categories

Executive Order 13526

Determination of Harm

Information may be classified if disclosure of the information reasonably could cause harm to national security or foreign policy.

Sec. 1.1(a)(4) – Classification Standards

Executive Order 13526

What kind of harm?

- CONFIDENTIAL – "damage"
- SECRET – "serious damage"
- TOP SECRET – "exceptionally grave damage"

Sec. 1.2 – Classification Levels

Executive Order 13526

Information may not be classified in order to:

1) Conceal violations of law, inefficiency, or administrative error;
2) Prevent embarrassment to a person, organization, or agency;
3) Restrain competition; or
4) Prevent or delay the disclosure of information that does not require national security protection

Sec. 1.7(a) – Classification Prohibitions and Limitations

Executive Order 13526

Markings Required by EO 13526

- Classified documents should contain:
  - Appropriate classification level
  - Identity of original classification authority
  - Identity of agency or office
  - Declassification instructions, including date or event for declassification
  - Concise reason for classification (Sec. 1.4)
- Portion Markings - 1.6(c)

Sec. 1.6 – Identification and Markings

Executive Order 13526

What about the other markings on the page?

- FOUO: For Official Use Only
- SBU: Sensitive But Unclassified
- LES: Law Enforcement Sensitive
- SSI: Sensitive Security Information
- CII: Critical Infrastructure Information
- CUI: Controlled Unclassified Information

Unclassified Information in Context: The Pieces of a Puzzle

Knowledge Preview

Ignacio, an intern for a national security agency, is tasked to create a report regarding international terrorism. He works with various officials in his agency to gather data, all unclassified, that he then compiles into a report.

As his superiors begin reviewing his work, they start to notice trends based on the way the information is compiled. A picture starts to develop, and there would be a harm to national security if the report became public…

Compilation Theory

- EO 13526 recognizes that when pieces of unclassified information are compiled into one document, they can create a classified picture.
- If this occurs, the compiled document may be classified.

Sec. 1.7(e) – Classification Prohibitions and Limitations

Knowledge Preview

Faisal, a FOIA professional at a national security agency, is processing a FOIA request for logs containing administrative tracking information. The tracking numbers in this log include a geographic abbreviation and are paired with dates. These numbers are not classified individually, and the compilation itself does not create a classified picture.

However, it occurs to Faisal that if a citizen paired the aggregated date and geographical information with information in the public domain, this could be the missing puzzle piece the citizen needs to do damage to national security.

Executive Order 13526

Mosaic Theory

- Courts have recognized that, at times, when pieces of unclassified information are paired with information already in the public domain, they can complete a classified picture.
- If this occurs, the unclassified, agency-controlled information may be classified and protected by Exemption 1.

Processing a FOIA Request & Exemption 1

Know Your Records!

- Does your agency maintain records containing classified information?
- What subject matters might this classified information generally relate to?

When Reviewing a FOIA Request…

- Ask yourself whether the request is seeking, either in whole or in part, classified information.
- Think about what records your agency might have and which repositories you may need to search.

Three Ways to Protect Classified Information Using Exemption 1

1. Glomar
2. Categorical
3. Apply Exemption 1 to specific information located in a search.

Three Ways to Protect Classified Information Using Exemption 1

Glomar

- Used when an agency determines that acknowledging the existence or non-existence of records would cause the harms of a particular FOIA exemption.

Original Glomar Response

"[The CIA Director] has determined that, in the interest of national security, involvement by the U.S. Government in the activities which are the subject matter of your request **can neither be confirmed nor denied**. Therefore, he has determined that **the fact of the existence or non-existence** of any material or documents that may exist which would reveal any CIA connection or interest in the activities of the Glomar Explorer is duly classified Secret in accordance with criteria established by Executive Order 11652."

Phillippi v. CIA, 546 F.2d 1009 (D.C. Cir. 1976)

Three Ways to Protect Classified Information Using Exemption 1

Categorical

- Used when:
  - An agency must acknowledge the existence of records (i.e. no Glomar), BUT
  - Agency can determine, without conducting a search, that all responsive records would be protected

Three Ways to Protect Classified Information Using Exemption 1

Application of Exemption 1 to Specific Information Located in a Search

- Mark and redact protected information
- NOTE: An agency has a duty to segregate and release all unclassified, non-exempt information.

Applying the Foreseeable Harm Standard

In accordance with the Department of Justice's 2022 FOIA Guidelines, agencies should confirm in their administrative response letters that they have applied the foreseeable harm standard when considering disclosure determinations.

Timing and Fixing Mistakes

Executive Order 13526

An agency may classify or re-classify information even after receiving a FOIA request. So long as…

- All substantive and procedural requirements are met;
- The classification process takes place with the "personal participation" or under the direction of the agency head, deputy agency head, or designated senior agency official; and
- The determination is made on a document-by-document basis.

Sec. 1.7(d) – Post-Request Classification

Executive Order 13526

If you locate classified records with deficient or conflicting markings…

- A classification authority within your agency may still evaluate the records to make a classification determination at the present time, and if the information is confirmed to be properly classified, it may be protected pursuant to Exemption 1.
- Deficient or conflicting markings may be corrected.

Knowledge Check

Fiona is a FOIA specialist with a Top Secret level security clearance. She has access to the paper files of a departed employee Dave who worked on sensitive matters. Upon conducting a FOIA search, she locates a folder labeled "Confidential." There are three pages inside, all responsive to the FOIA request, and none have any classification markings.

How should Fiona proceed in processing this FOIA request?

*Disregard the potential application of any FOIA exemptions, except for Exemption 1.

Waiver of Exemption 1

Waiver of Exemption Protection

- Plaintiff bears the burden
- Waiver only if the requested information is (1) as specific as the released information; (2) matches the released information; and (3) has been made public through an official and documented disclosure.

Fitzgibbon v. CIA, 911 F.2d 755 (D.C. Cir. 1990)

Waiver of Exemption Protection

- The Fitzgibbon test also applies in the *Glomar* context
  - In this context, the "released information" referenced in the test would be information regarding the existence of the requested records.

Waiver of Exemption Protection

For Waiver, Official Disclosures Must Come From:

- The President, those acting at the direction of the President, or the agency asserting Exemption 1.
  - One component in the agency can waive for the whole agency, but a sister agency cannot waive for other agencies.
  - Statements by former officials are not official disclosures, nor are unauthorized leaks.

Declassification Provisions of EO 13526

Executive Order 13526

"No information may remain classified indefinitely"

Declassification Timeline:

- Specific date or event
- 10 years after classification decision
- 25 years if justified by sensitivity of information
- 75 years if reveals confidential human source, human intelligence source, or design concepts of weapons of mass destruction

Sec. 1.5 – Duration of Classification

Executive Order 13526

Sec. 3.3 – **Automatic Declassification**

- 25 years or older, of permanent historical value, but not necessarily reviewed before declassification

Sec. 3.4 – **Systematic Declassification**

- Systematic declassification review should occur for records exempted from automatic declassification, and which have permanent historical value

Executive Order 13526

Sec. 1.8 – **Classification Challenges**

- Government officials who are authorized holders of information and who believe, in good faith, that classification is improper may challenge that classification

Sec. 3.5 – **Mandatory Declassification Review**

- Request from public for declassification of specific documents

Executive Order 13526

Can information be classified even after it has been declassified and released?

No, unless strict criteria are met:

- Document-by-document review that reclassification is required to prevent "significant and demonstrable damage to national security"
- Personally approved in writing by agency head
- "Reasonably recoverable" without bringing undue attention to information
- Must be reported to Information Security Oversight Office (ISOO)

Sec 1.7(c) – Reclassification After Release

Litigation Considerations

Defending Exemption 1 in Litigation

Standard of Review

- National security officials are uniquely positioned to view "the whole picture" and "weigh the variety of subtle and complex factors" in order to determine whether the disclosure of information would damage national security.

CIA v. Sims, 471 U.S. 159, 179-80 (1985).

Defending Exemption 1 in Litigation

Standard of Review

- "Expansive standard of deference"
- "[L]ittle proof or explanation is required beyond a plausible assertion that information is properly classified."

Morley v. CIA, 508 F.3d 1108, 1124 (D.C. Cir. 2007).

Defending Exemption 1 in Litigation

Before the bench

- Federal Judges have automatic clearance
- May order an in camera review
- Generally "the court will not conduct a detailed inquiry to decide whether it agrees with the agency's opinions."

Edmonds v. DOJ, 405 F. Supp. 2d 23, 29 (D.D.C. 2005).

Defending Exemption 1 in Litigation

Agency affidavits are key to success

- Affiant must have direct knowledge of classification decision
- Reasonably specific and no evidence of bad faith
- Provide as much information as possible without disclosing classified information

Questions?