Sensitive Information on the Web, an Information Security Perspective

Ray Holmer

STIP Meeting

May 1, 2003

Background

- Blake Memorandum – Oct. 26, 2001
- White House WMD Memorandum – March 19, 2002
- Secretary WMD Memorandum – May 30, 2002
- Web sites seen as terrorists aids
- Internet Content Advisory: Considering the Unintended Audience

More Recent Developments

- Executive Order 13292 re: Classified National Security Information – Mar. 25, 2003
- DOE OUO directives - Apr. 9, 2003
  - DOE O 471.3, Identifying and Protecting Official Use Only Information
  - DOE M 471.3-1 Manual for Identifying and Protecting Official Use Only Information
  - DOE G 471.3-1, Guide to Identifying Official Use Only Information

Current Guidance

- The policy letter directing DOE and NNSA to review unclassified information for sensitivity is still in effect.
- The White House direction for all Federal Agencies to review and continue to review unclassified information related to Weapons of Mass Destruction (Nuclear, Chemical, Biological, and Radiological) to ensure that information being broadly released is not useful to terrorists is still in effect.
- The new OUO order helps to reinforce this.
- Additionally, OPSEC, Export Control, and UCNI reviews have always been required.

Information Availability

- Material removed from sites is still available:
  - Web Archives
  - Search Engines
  - Other
- Solution: Do not place sensitive information on Web sites.

Application to STI

- Balance value to science of disseminating versus need to protect against risk (agency mission)
- Continue to follow existing review requirements and the STI model (checklist of statutory bases for limitations to access)
- Incorporate as appropriate to your organization the latest guidance, such as OUO, EO, and programmatic guidance
- Mark STI documents and DOE Form 241.1 consistently

Potentially Sensitive Information

- Facilities, Personnel
- Programs, Materials
- Security, Safety
- Assessments, Vulnerabilities
- Sensitive Subjects List

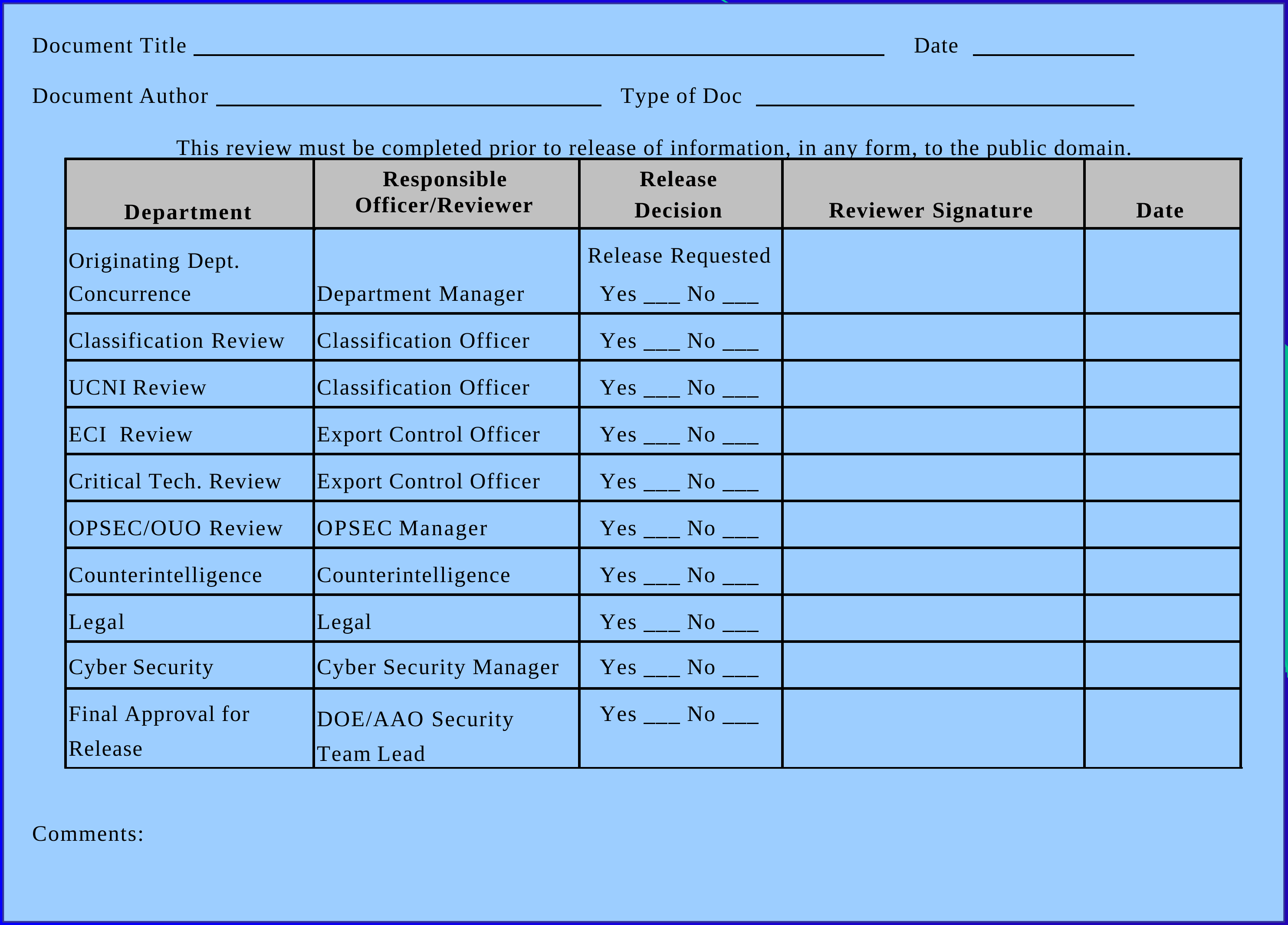
Considerations

- Suitability – What does it do for the person, organization, Department?
- Sensitivity – How can it be used by an adversary?
- Risk – What are the chances of an adversary using the information?
- Consequences – What could happen if an adversary used the information?

Review Process

- Team Approach
- Suitability – Organization, program
- Sensitivity – Facility Security, OPSEC, Classification
- Risk – CN, OPSEC, Facility Security
- Consequences – All
- Conflict Resolution by Senior Management

One Approach



Document Title ____ Date __________

Document Author __________________________ Type of Doc __________________________

This review must be completed prior to release of information, in any form, to the public domain.

Department	Responsible Officer/Reviewer	Release Decision	Reviewer Signature	Date
Originating Dept. Concurrence	Department Manager	Release Requested Yes ___ No ___		
Classification Review	Classification Officer	Yes ___ No ___		
UCNI Review	Classification Officer	Yes ___ No ___		
ECI Review	Export Control Officer	Yes ___ No ___		
Critical Tech. Review	Export Control Officer	Yes ___ No ___		
OPSEC/OUO Review	OPSEC Manager	Yes ___ No ___		
Counterintelligence	Counterintelligence	Yes ___ No ___		
Legal	Legal	Yes ___ No ___		
Cyber Security	Cyber Security Manager	Yes ___ No ___		
Final Approval for Release	DOE/AAO Security Team Lead	Yes ___ No ___		

Comments:

The Reality

- There is no definitive list of what shouldn't be broadly published.
- Decisions will still need to be based on the positive aspects of broad publication vs. the negative consequences of assisting terrorists in making rapid advances.

Questions

Contact:

Ray Holmer, Program Manager

Technical and Operations Security

Safeguards and Security Policy Staff

SO-113

Phone – 301-903-7325

E-mail – raymond.holmer@hq.doe.gov