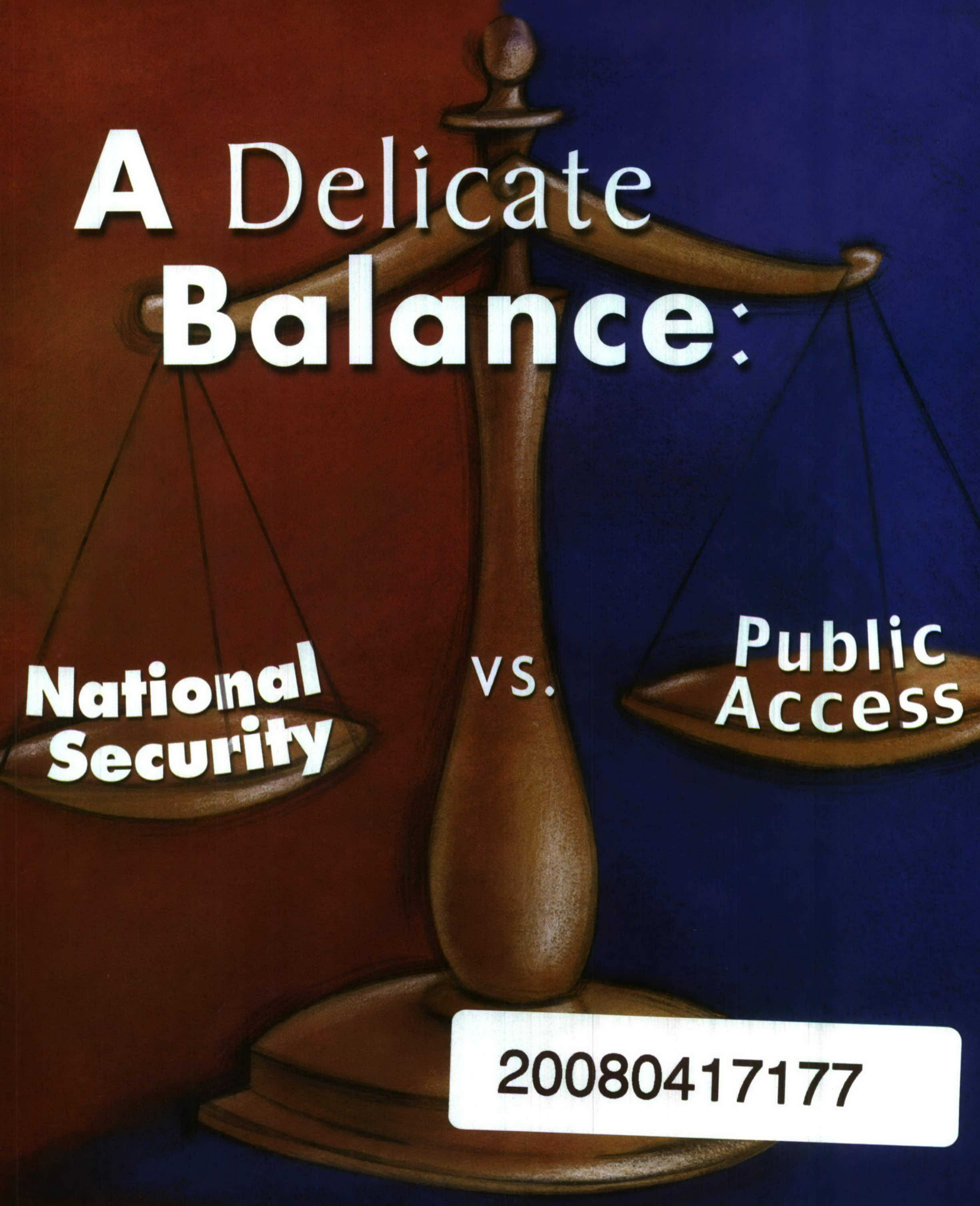

BY BONNIE KLEIN AND SANDY SCHWALB

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
March 2005	Journal Article	April 2005

4. TITLE AND SUBTITLE
A Delicate Balance: National Security vs. Public Access

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Klein, Bonnie; Schwalb, Sandy

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
8725 John J. Kingman Road
Ft. Belvoir, VA 22060-6218

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Technical Information Center
8725 John J. Kingman Road
Ft. Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)
DTIC

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES: Published in Computers in Libraries, Vol.25 No. 3, April 2005, p.16-23. U.S. Government Work.

14. ABSTRACT

In the aftermath of September 11, 2001, the Defense Technical Information Center (DTIC-http://www.dtic.mil) found itself in the spotlight as journalists, academics and policy-makers sounded the alarm on both sides of the issue of public access to scientific and technical government information; namely, too much access and not enough access. This article explains the issues, policies, decisions and processes that led to the withdrawal of some government information from public release.

15. SUBJECT TERMS:
Federal Information Policy; Information Centers, Defense Technical Information Center

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Bonnie Klein
UU	UU	UU	UU	6	19b. TELEPHONE NUMBER *(include area code)* 703 767-8037

SCAN: Pages 16, 17, 18, 20, 22, 23

Sometimes people want to see data that the government thinks should be kept under wraps. How does the Department of Defense balance the scales of justice while still ensuring information security?

In the aftermath of September 11, 2001, the Defense Technical Information Center (DTIC—http://www.dtic.mil) found itself in the spotlight as journalists, academics, and policy-makers sounded the alarm on both sides of the issue of public access to scientific and technical government information; namely, too much access and not enough access. Since we worked there at the time, we saw what was going on and why. In the interest of helping people understand what is happening to government information in the wake of terrorist concerns, we want to explain the processes and the decisions that have been involved in the withdrawal of some government information from public release.

What Is DTIC's Function?

DTIC was established in 1945 as the Air Documents Division to collect and catalog World War II scientific and technical documents, including information gathered from the European and Pacific Theaters of War. Today it is the centralized repository and secondary disseminator of scientific and technical information (STI) produced by or for the Department of Defense (DoD) research, development, testing, and engineering programs.

By accepted definition, DTIC is a repository of "gray literature." Most of our documents are not available through normal publishing or distribution channels. The technical reports in our collection have been produced in small quantities for primary distribution to recipients specified by the DoD organization that sponsored, supported, or received the work on behalf of the DoD.

Categories of Information

The DoD's scientific and technical information is always categorized, or "marked" (the term used by the defense community) by the office that originates the document to show its level of sensitivity and to whom the document can be distributed. Guidelines and authorized reasons to limit DoD STI distribution have been in place since 1983. (See the sidebar "Reasons for Limited Distribution.")

The content provider or responsible DoD organization that generates the document and has the best knowledge of its technical content makes the initial determination. The markings are vetted by any or all of the following within the originating agency or provider: the Project Manager, the Contracting Office, Public Affairs Office, Security Office, Foreign Disclosure Office, and the Scientific and Technical Information Office.

Here are the classifications commonly used by the DoD:

Classified, Limited Distribution: Some information is classified to protect national security; in January 2004, 7 percent of DTIC's collection was in this category. The other 93 percent was unclassified.

Unclassified, Limited Distribution: Although not Classified, information may still be sensitive for various reasons. Forty percent of DTIC-held documents are "Unclassified, Limited" and include information that may be exempt from public release under the Freedom of Information Act (FOIA).

Unclassified, Unlimited Distribution: It is DoD policy to maximize the availability of technical information and products resulting from Defense-funded research consistent with restraints such as national security, export control, and intellectual property rights. The goal is to foster technology transfer and the overall advancement of science. In keeping with that policy, 53 percent of DTIC's collection is "Unclassified, Unlimited" and available "for public release" to anyone anywhere, even to our adversaries who we know cull and exploit public release information for intelligence purposes. Of course, we know that this is a by-product of our open society. For example, an Al Qaeda training manual recovered in Afghanistan states: "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of information about the enemy." A Chinese military intelligence manual published in the early 90s is a how-to guide on gathering useful

»

information from U.S. Government public sources—and this was before the Internet made it easy and low-cost.

DTIC as Data Gatekeeper

DTIC controls access to DoD Classified and Unclassified, Limited information through a registration process. Our primary customers are those who have a legitimate business relationship with DoD. Those registered users, of course, include the military and contractors. In addition, our 2003 Customer Satisfaction Survey found that a majority of our users are librarians, engineers, and researchers.

You are eligible to register if you fit one of these categories:

- are an employee of a DoD organization (civilian and military including National Guard and Reserves on active duty), DoD contractor, or potential DoD contractor
- are an employee of another U.S. Federal Government agency or U.S. Federal Government contractor
- are a researcher of a university or college funded by DoD or a U.S. Federal Government agency for conducting research throughout the U.S.

Reasons for Limited Distribution of Scientific and Technical Information

From DoD Directive 5230.24, Distribution Statements on Technical Documents
http://stinet.dtic.mil/stinfo/data/DoDD_523024.pdf

Foreign Government Information
To protect and limit distribution in accordance with the desires of the foreign government that furnished the technical information.

Proprietary Information
To protect information not owned by the U.S. Government and protected by a contractor's "limited rights" statement, or received with the understanding that it not be routinely transmitted outside the U.S. Government.

Critical Technology
To protect information and technical data that advance current technology or describe new technology in an area of significant or potentially significant military application or that relate to a specific military deficiency of a potential adversary. Information of this type may be classified or unclassified; when unclassified, it is export-controlled.

Test and Evaluation
To protect results of test and evaluation of commercial products or military hardware when such disclosure may cause unfair advantage or disadvantage to the manufacturer of the product.

Contractor Performance Evaluation
To protect information in management reviews, records of contract performance evaluation, or other advisory documents evaluating programs of contractors.

Premature Dissemination
To protect patentable information on systems or processes in the developmental or conceptual stage from premature dissemination.

Administrative or Operational Use
To protect technical or operational data information from automatic dissemination under the International Exchange Program or by other means. This protection covers publications required solely for official use or strictly for administrative or operational purposes. This statement may be applied to manuals, pamphlets, technical orders, technical reports, and other publications containing valuable technical or operational data.

Specific Authority
To protect information not specifically included in the above reasons and discussions, but which requires protection in accordance with valid documented authority such as Executive Orders, classification guidelines, DoD or DoD Component regulatory documents.

Direct Military Support
To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD approved activities may jeopardize an important technological or operational military advantage of the United States.

Export Control
To protect technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979 (Title 50, U.S.C., App. 2401 et seq.), as amended. Violations of these export laws are subject to severe criminal penalties.

- are a participant in the Small Business Innovation Research or Small Business Technology Transfer (SBIR/STTR) program
- are a faculty member, staff member, or student of Historically Black Colleges and Universities (HBCU), Hispanic Serving Institutions (HSI), Tribal Colleges and Universities (TCU), and other Minority Institutions (MI)

Serving the Information Community and the Public

DTIC was an early pioneer in the use of the Internet for information dissemination. Among the 100-plus Web sites hosted by DTIC are its own information holdings as well as numerous sites sponsored by components of the Office of the Secretary of Defense, military service headquarters organizations, and several defense agencies.

"In the wake of September 11, 2001, the way in which Federal Government agencies disseminated their information changed very little."

Because DTIC collects and does not produce the information in our collection, the military technical reports are not available through the Government Printing Office's Federal Depository Library Program (GPO-FDLP). DTIC's conduit to libraries, the broader scientific community, and the public at large is the National Technical Information Service (NTIS) http://www.ntis.gov.

In the early 1970s, DTIC was on the leading edge of computer technology in offering our registered users online access to bibliographic services. In 1994, information technology advances made it possible for DTIC to offer this service directly to the public with the launch of DTIC's Scientific and Technical Information Network (STINET). In April 1998, we added the capability to link from new citations to the full text. As of February 2004, Public STINET http://stinet.dtic.mil offered free online access to over 115,000 full-text, public-release documents, as well as 347,000 citations to older documents that are not digitized.

After September 11, 2001

An April 2002 Congressional Research Service (CRS) report, *Possible Impacts of Major Counter Terrorism Security Actions on Research, Development, and Higher Education*[1] states that: "Since September 11, 2001, the Government has imposed increased rigorous controls on access to scientific and technical information that could be of potential value to terrorists."

The report makes a salient point in the beginning: "Science and technology (S&T) are a double-edged sword in the fight against terrorism—whether at home or abroad. S&T can help prevent and attenuate attacks (communications, surveillance and prevention technologies, public health vaccines, and pharmaceuticals) and defend against enemies (by strengthening the arsenal of weapons). But S&T can benefit the terrorist by providing advanced technologies or weapons—nuclear, chemical, biological and cyber—by giving terrorists opportunities to purchase information and products to exploit the vulnerabilities of complex technological systems on which advanced economies depend. ..."

The CRS report mentions two *New York Times* articles that appeared in early 2002. The first article, from Jan. 13, headlined, "U.S. Selling Papers Showing How to Make Germ Weapons,"[2] caught the eye of policy-makers in Washington. It stated, "Today, the germ reports declassified by military officials are made available to the public by the Defense Technical Information Center ... the Pentagon's main repository of scientific and technical data, which has a comprehensive Web site that helps identify old documents."

Science and technology can help prevent attacks, but they can also help terrorists.

The second article, which appeared on Feb. 17, reported that the Bush administration "has closed public access to over 6,600 technical reports dealing with biological and chemical weapons production."[3] In fact, those "6,600 technical reports" were mostly citations with no full text associated with them and DTIC removed them from our STINET at the end of January 2002.

We found the manner in which the media covered these activities quite interesting. They reported about information that was readily available to the public and could be used by terrorists, and then reported when this same information was removed from government Web sites and public distribution. In both cases, the media found the government actions alarming!

DTIC and the 'Card Memo'

In January 2002, DTIC developed multiple search strategies to identify CBRN documents: those relating to

»

chemical, biological, radiological, and nuclear weapons, and to temporarily withdraw them from public access until a review of the documents was completed. In fact, DTIC managers discussed the situation and issues to be considered with those drafting a White House directive, which was released on March 19. This memo, "Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security," was released by Andrew H. Card Jr., who carried the titles of Assistant to the President and Chief of Staff at the White House.[4]

"Government agencies routinely review documents and make changes. In fact, it is through this type of process that classified documents become declassified."

Referred to as the "Card Memo," it directed all executive departments and agencies to use existing policies and procedures for identifying and safeguarding all information pertaining to the development or use of CBRN that could be misused to harm the security of our nation or threaten public safety. This memo did not set new policy, but reminded department and agency officials about the processes already in place for the classification, reclassification, and declassification of government information. (See Figure 1.)

Here's the Way Our Review Process Worked

There are two stages to our review process:

Step 1: Identification—DTIC's Reference and Retrieval staff, which includes librarians and technical information specialists, worked in collaboration with DoD scientists and subject matter experts to pinpoint the DTIC thesaurus descriptors and identifiers used to build our citation search strategy. Our goal was to identify only those public-release documents that dealt with CBRN weaponization. This task took a week to complete and netted the 6,600 citations withdrawn from DTIC's Public STINET in late January 2002. It should be noted that those 6,600 citations came from a collection of more than 1 million public-release documents and was therefore a narrow subset of the data that was under review.

Step 2: Content Evaluation—DoD military classification experts are examining the documents to determine if they should once again be made available to the public, be reclassified or put in the category of Unclassified, Limited information. The documents are about work done primarily between the 1940s and 1960s and declassified in the 1970s. The majority of the documents are from the Army, which did most of the chemical-biological research over the last 60 years.

The content review phase is an ongoing process. Government agencies routinely review documents and make changes. In fact, it is through this type of process that classified documents become declassified.

Withdrawn, Not Gone: A Delicate Balancing Act

What we want to emphasize is that the information withdrawn from public release is still accessible directly from the DoD to legitimate DoD customers and users who are eligible to register for

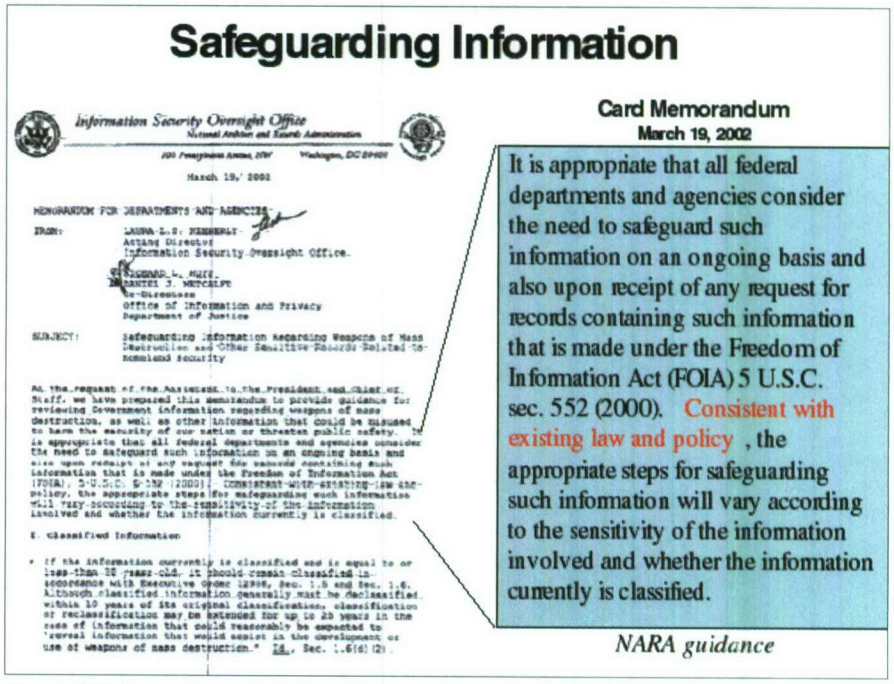

Figure 1: This is from a DTIC overview presented by Nancy Wright, Director, (DTIC) User Services Directorate, in March 2003.

DTIC services—this includes government contractors, potential contractors, and grantees.

In the wake of September 11, 2001, the way in which Federal Government agencies disseminated their information changed very little.

In 2000–2001, the U.S. National Commission on Libraries and Information Science (NCLIS) examined the thorny issues related to public information dissemination, which led to a report that came out in the spring of 2001. In the section on federal agency needs for central Information Services and Information Management, it states:

> Agencies are continually confronted with the challenge of balancing the public's right to know against the government's obligations to protect proprietary, privacy, and national security information. Agencies must also be sensitive to the need to preserve the integrity of the content of their information. One must realize that the government is not a monolithic entity. It is comprised by many organizations with a wide range of interests and relationships. Most government policies address either the control of information or making it available to the public.[5]

The balance between national security and public access is a delicate one. Debates about controls on government information have been going on for decades. Those who remember "the old days" when government documents could be found only in paper know that these issues will continue to be discussed as more and more information becomes available in electronic form only.

Newly generated government information will be evaluated against established criteria for review for public release, the same as always. This is a decentralized process. There is no core group making these decisions, although there may be a tendency on the part of those responsible to err on the side of caution.

A report released in June 2003 from the National Archives and Records Administration, Information Security Oversight Office, (*2002 Report to the President*) recognizes that this debate is necessary. It states:

> Our Nation and our Government are profoundly different in a post 9/11 world. Americans' sense of vulnerability has increased, as have their expectations of their Government to keep them safe. Information is crucial to responding to these increased concerns and expectations. On the one hand, Americans are concerned that information may be exploited by our country's adversaries to harm us . . . (however) the free flow of information is essential if citizens are to be informed and if they are to be successful in holding the Government and its leaders accountable. In many ways, the Federal government is confronted with the twin imperatives of information sharing and information protection, two notions that contain inherent tension but are not necessarily contradictory. While great emphasis is often placed on the consequences of the improper disclosure of classified (or unclassified) information, restrictions on dissemination of information carry their own risks. Whether within the Federal Government or between the Federal Government and state, local and private sector personnel, or with the public, the ability to share information rapidly and seamlessly can make the difference in precluding or responding to the next terrorist event.[6]

Bonnie Klein is a technical reports team leader in the Information Collection Division at the Defense Technical Information Center in Ft. Belvoir, Va. She holds an M.L.S. from the University of Illinois–Urbana-Champaign and an M.S.Ed. in instructional systems technology from Indiana University–Bloomington. Her e-mail address is bklein@dtic.mil. When this article was written, Sandy Schwalb was a marketing specialist with DTIC. She is now DTIC's public affairs officer. She holds a B.A. in history from (as it was then known) the State University of New York–Binghamton. Her library expertise comes from her 10 years with the Special Libraries Association and 5 years at the Government Printing Office. Her e-mail address is schwalb@dtic.mil. Both authors have been actively involved with the Federal Library and Information Center Committee (FLICC) and both have written extensively and made presentations about government information policies and practices.

References

1. Knezo, Genevieve J., *Possible Impacts of Major Counter Terrorism Security Actions on Research, Development, and Higher Education,* Congressional Research Service, April 8, 2002. http://www.aau.edu/research/crsterror.pdf
2. Broad, William J., "U.S. Selling Papers Showing How to Make Germ Weapons," *New York Times*, Jan. 13, 2002.
3. Broad, William J., "U.S. Tightening Rules on Keeping Scientific Secrets," *New York Times*, Feb. 17, 2002.
4. White House Chief of Staff Memo, "Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security," March 19, 2002. http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm
5. U.S. National Commission on Libraries and Information Science, *Comprehensive Assessment of Public Information Dissemination June 2000 - March 2001 Appendix 24: Panel Two: Final Report on Federal Agency Needs for Central Information Services and Information Management.* http://www.nclis.gov/govt/assess/assess.appen24.pdf
6. National Archives and Records Administration, Information Security Oversight Office, 2002 Report to the President, *A Look to the Future of the Security Classification System in a Post 9/11 Environment.* June 30, 2003. http://www.archives.gov/isoo/annual_reports/2002_annual_report.html#post911