

~~FOR OFFICIAL USE ONLY~~

DOCUMENT NO. IAFI-UDCI-STG-001
25 MAR 2002

(b) (3)
(b) (5)
(b) (7) (e)

Interagency Task Force Report

on

Unauthorized Disclosure of Classified Information

Science & Technology Working Group

Chaired by

Central Intelligence Agency Directorate of Science and Technology

March 25, 2002

25

~~FOR OFFICIAL USE ONLY~~

APPROVED FOR RELEASE
DATE: FEB 2007

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1
Conclusions 1
Recommendations 2
1.0 SCOPE..... 3
1.1 Directive 3
1.2 Background..... 3
1.3 Mission 4
2.0 UNAUTHORIZED DISCLOSURE PROCESS..... 5
2.1. Unauthorized Disclosure 5
2.2 Unauthorized Disclosure Investigation..... 6
3.0 TECHNOLOGY ASSESSMENT..... 7
3.1 Previous Studies 7
3.2 Digital File Management and Control 8
3.2.1 DRM: [REDACTED] 8
3.2.2 Auditing Network Activity: [REDACTED] 10
3.3 Paper Document Management and Control..... 12
3.3.1 Watermarks 12
3.3.2 Word- or Version-Encoding..... 12
3.3.3 Digital Books 12
3.3.4 Electronic Document Tags (eTags)..... 13
3.3.5 Compressed-Image File Capture..... 13
3.4 Auditing Open Sources..... 13
3.5 Emerging Technology Threats 13
4.0 CONCLUSIONS..... 15
APPENDIX A: REFERENCE DOCUMENTS..... 16

LIST OF FIGURES

FIGURE 1: PROCESS DIAGRAM OF UNAUTHORIZED DISCLOSURE 5
FIGURE 2: PROCESS DIAGRAM OF UNAUTHORIZED DISCLOSURE INVESTIGATION 6
FIGURE 3: INTELTRUST SYSTEM ARCHITECTURE DIAGRAM 9

LIST OF TABLES

TABLE 1:

 FEATURES AND BENEFITS 11

EXECUTIVE SUMMARY

- (U) In January 2002, the United States Attorney General established an interagency task force to conduct a comprehensive review of current protections against the unauthorized disclosure of classified information to the media (*i.e.*, "leaks"). The Science and Technology Working Group (S&TWG), one of four Working Groups the task force created to support this effort, was charged with evaluating scientific and technical solutions to this issue.
- (U) The S&TWG reviewed past and current technical methods to manage and control the dissemination of classified information from a cleared individual, with authorized access to the information, to the media. The S&TWG also assessed the impact of emerging and future technologies on existing processes and controls
- (U) The S&TWG evaluated a number of commercial applications (specifically, systems developed to improve security and controls in e-business) for their potential to improve management and control of classified information in a classified environment. The S&TWG also explored processes and technology to increase the level of "deterrence" against unauthorized duplication and dissemination of classified information. Finally, the Working Group assessed the potential threats of emerging commercial technologies migrating into the classified workplace.

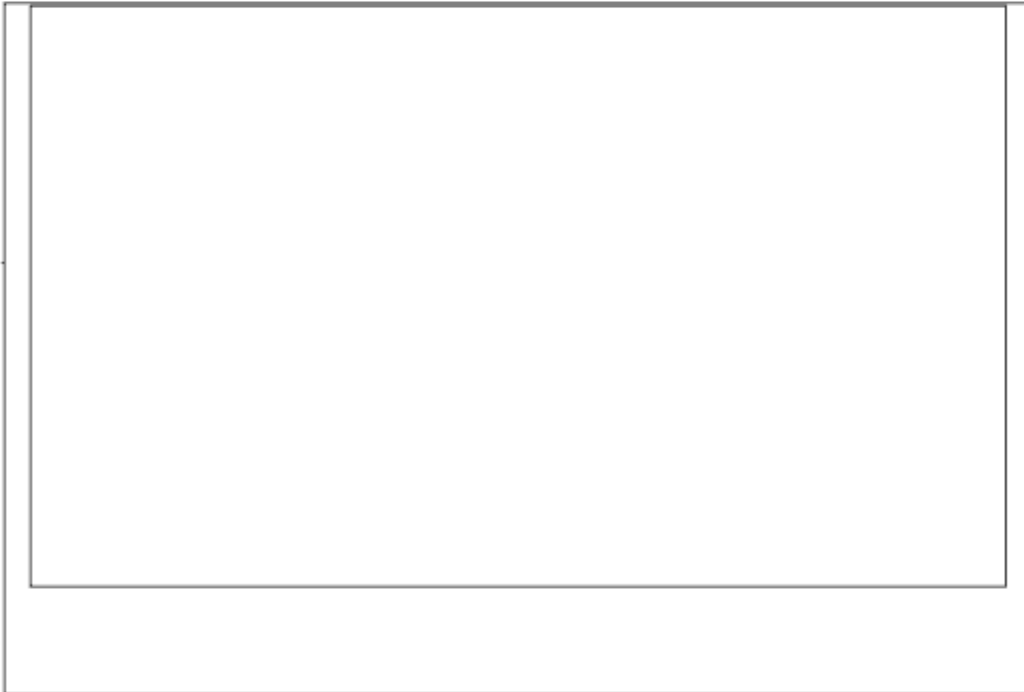
Conclusions

- (U) The S&TWG drew the following conclusions about scientific and technical tools that can improve the management and control of classified information:
1. (U) **Key Finding:** There is no scientific or technical system or systems that can unequivocally prevent the dissemination of classified information from someone cleared to have it to someone without "need to know." However, the exponential growth of digital data in the work environment has been paralleled by the development of sophisticated tracking and audit technologies that can make it extremely difficult to move classified information out of the classified environment. It is possible to close the gaps in control of such information so that the only methods of transporting it beyond the classified environment are verbally or through personal notes.
 2. **Digital File Management and Control:** Commercially available Digital Rights Management (DRM) technology can provide effective control of classified information on a classified network.
 3. **Auditing Network Activity:** Commercially available tools for auditing network and telecommunications activity can be implemented within a classified environment to flag unauthorized activity and, when necessary, support after-the-fact investigation of unauthorized disclosure.
 4. **Paper Document Management and Control:** The ability to photocopy documents for unauthorized distribution can be substantially reduced by replacing stand-alone copiers with networked copiers that incorporate scanner/printer technology, which allows the network to audit activity, take control of a document, and prevent its unauthorized duplication.

5. **Emerging Technologies in the Workplace:** Wireless technologies, digital cameras, personal digital assistants and other emerging technologies must be carefully assessed before they are permitted into the classified workplace.

Recommendations

~~(FOUO)~~ The S&TWG makes the following recommendations to improve the management and control of classified information and prevent its dissemination beyond the classified environment:



1.0 SCOPE

1.1 Directive

- (U) On January 21, 2002, the Attorney General convened an interagency task force to conduct a comprehensive review of current protections against the unauthorized disclosure of classified information. In forming this task force, the Attorney General was in consultation with the Secretaries of the Department of Defense (DOD), Department of State (DOS), Department of Energy (DOE), Central Intelligence Agency (CIA), and others. To support this initiative, the Attorney General and Counsel appointed a Steering Committee, Committee of Group Chairs and four (4) Working Groups to address litigation, legislation, science and technology, and security issues.
- (U) The Science & Technology Working Group (S&TWG) was charged with reviewing technical capabilities to track and control classified information. The S&TWG was also tasked to assess ways in which science and technology can assist in the investigation of classified information leaks.
- (U) The S&TWG was chaired by the CIA/Directorate of Science and Technology (DST) and included representatives of the Department of Justice (DOJ), Federal Bureau of Investigation (FBI), DOD, DOE, DOS, National Security Agency (NSA) and National Reconnaissance Organization (NRO).

1.2 Background

- (U) All United States Agencies handling classified information have policies and procedures in place to restrict its dissemination to cleared individuals on a "need-to-know" basis. While the overall effectiveness of these measures is not quantified, there have been previous calls for review. Testifying before the Senate Select Committee on Intelligence (SSCI) in August 2000, the Director of Central Intelligence (DCI) requested that all Agencies in the Intelligence Community (IC) review their personnel and security programs, including those intended to prevent the unauthorized disclosure of classified information.
- (U) As evidenced by the creation of this task force, leaks continue to occur. Furthermore, leaks are nearly impossible to predict; and without physical evidence, they are extremely difficult to trace back to the responsible individual.
- (U) People leak information for any number of reasons: negligence, by accident, as an act of espionage, or as willful disclosure to satisfy some personal need. Education can reduce negligence. Well-designed control mechanisms and work processes can minimize the accidental leak. Countering a well-planned, focused technical or human espionage operation is more difficult, as system vulnerabilities are systematically exploited. The willful disclosure by one with authorized access may be the most difficult leak to manage via technical controls. Individual motivation can be mitigated somewhat by "deterrents," i.e., the use of technical interventions, psychological and behavioral threats that generate fear of detection and reprisal. But even the most sophisticated technology cannot prevent the authorized individual, intent on leaking, from memorizing or hand-copying information and passing it to an unauthorized person.

1.3 Mission

(U) The S&TWG focused on identifying scientific and technical tools to stop the willful disclosure of classified information to the media. Specifically, the Working Group:

- (U) Reviewed available scientific and technical applications and tools to control and track access to, and dissemination of, classified government information;
- (U) Assessed ways in which technology can assist in the investigation of unauthorized disclosures;
- (U) Identified emerging and anticipated developments in science and technology that will require changes to existing and proposed protections against unauthorized disclosure.

1.4 Fundamental Assumptions

(U) The S&TWG adopted the following assumptions as fundamental to its analysis:

1. (U) Leakers have authorized access to the classified information they leak.
2. (U) Leakers are deterred by technologies they perceive as being effective.
3. (U) Keeping highly effective technologies a secret will inhibit Leakers' ability to exploit vulnerabilities.
4. (U) Scientific and technical deterrents can be defeated, given enough time and resources.
5. (U) Technical solutions to limiting unauthorized dissemination of classified information must be integrated into the comprehensive system of existing technologies, processes, organizational cultures and individual behaviors unique to the agency where they are to be implemented.

2.0 UNAUTHORIZED DISCLOSURE PROCESS

(U) In a systematic approach to fulfilling its mission, the S&TWG dissected both the process that leads to an unauthorized disclosure of classified information, and the after-the-fact investigative process to identify the responsible person. The Working Group then targeted areas for technical intervention and began to explore applicable scientific and technical solutions.

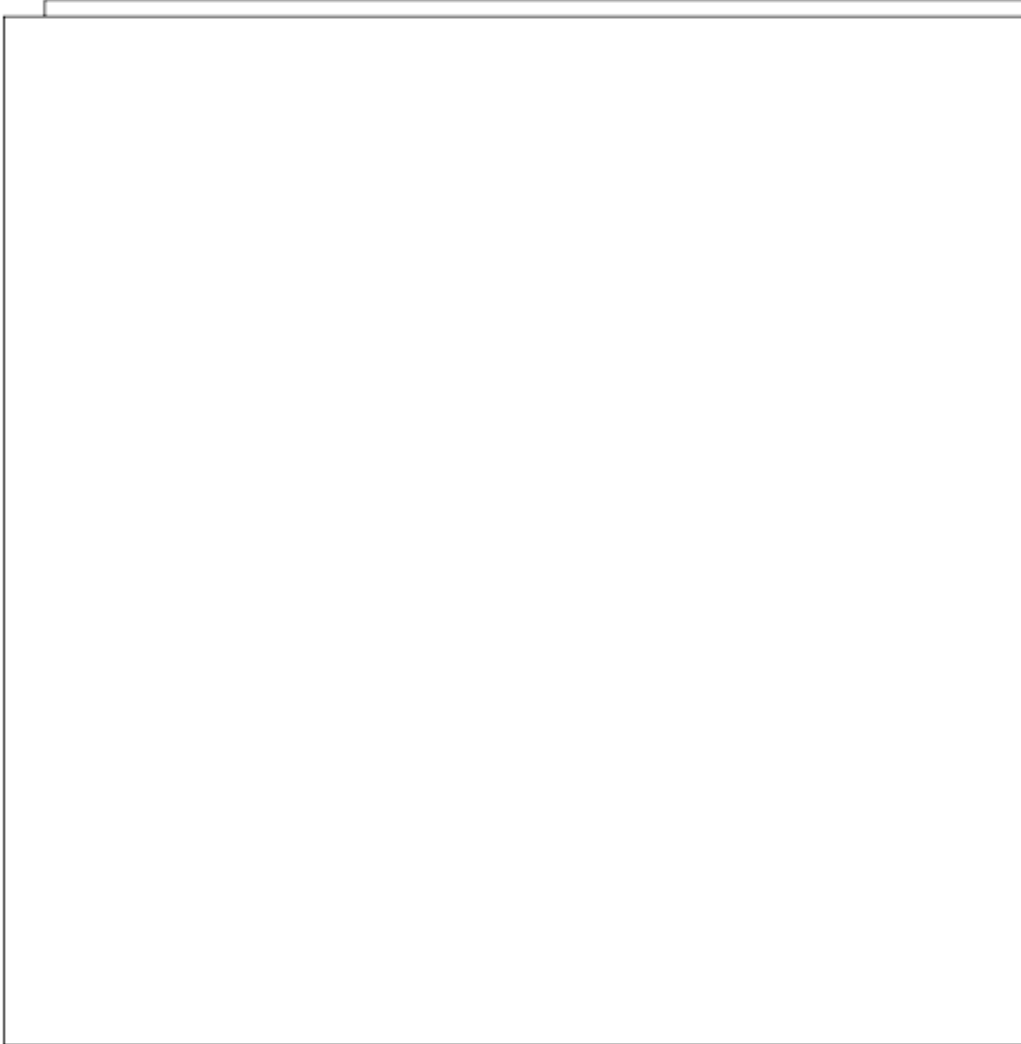
2.1. Unauthorized Disclosure



~~FOR OFFICIAL USE ONLY~~

DOCUMENT NO. IAFT-UDCI-STG-001
25 MAR 2002

2.2 Unauthorized Disclosure Investigation



~~FOR OFFICIAL USE ONLY~~

3.0 TECHNOLOGY ASSESSMENT

- (U) The S&TWG members assessed their respective Agencies for studies, pilots, research reports and other sources of information on scientific and technical tools, applications and processes to control and track the flow of classified information.

3.1 Previous Studies

- (U) From 1995 to 2000, the CIA Directorate of Science and Technology (DST) Office of Research and Development (ORD) wrote a series of reports on potential technical solutions to improving classified information management. These reports were reviewed and a number of initiatives identified within the CIA, In-Q-Tel (the CIA's venture capital activity), and the Directorate of Operations (DO) [redacted] which has undertaken efforts to make classified CIA documents and highly sensitive finished intelligence, including the President's Daily Brief (PDB), more secure.
- (U) Among the least effective methods for preventing unauthorized dissemination of classified documents are copier-management systems that use devices attached to standard photocopiers, or require biometric ID or PIN entry for access. In ORD's assessment (and the S&TWG concurs), these systems do not prevent authorized users from copying for illicit purposes. Their only benefit may be as a deterrent, i.e., users perceive their presence as a risk.
- (U) CIA/ORD assessed the viability of using special inks with copiers to degrade copy quality to the point it becomes illegible. Specifically tested were the use of photochromic inks, which change contrast under high illumination, and thermochromic inks, which change contrast under thermal loading. Unfortunately, extensive testing on copiers of the time had limited success in effectiveness and reliability. The change in copier design over the past several years, from xerography technology to a combination of scanner/printer technology, resulted in reductions in light intensity and operating temperatures that leave special inks even less effective. Moreover, the contrast-change effect was easily defeated when the type of ink was known; e.g., thermochromic ink can be circumvented by "chilled" paper.
- (U) CIA/ORD also documented evaluations of optical techniques that used highly reflective surfaces to produce either blank or corrupted copies of an original document. The concept was immature and showed little promise. A significant detriment to the viability of this technique is the requirement that standard paper be replaced with a special reflective product.
- (U) CIA/ORD looked at exploiting efforts in the security printing industry to authenticate and prevent forgery of financial documents, contracts, notes, etc., but concluded that, "None of these technologies are believed capable of preventing a person dedicated to copying the document for purposes of leaking the information from discovering the relatively simple countermeasures that would permit the protected document to be copied."
- (U) CIA/ORD reported more encouraging findings about controlling access to, and distribution of, electronic data. Indeed, its Document Security Program report issued in 2000 stated that, "Electronic document dissemination offers the hope for eliminating many of the security vulnerabilities associated with hard copy document dissemination."

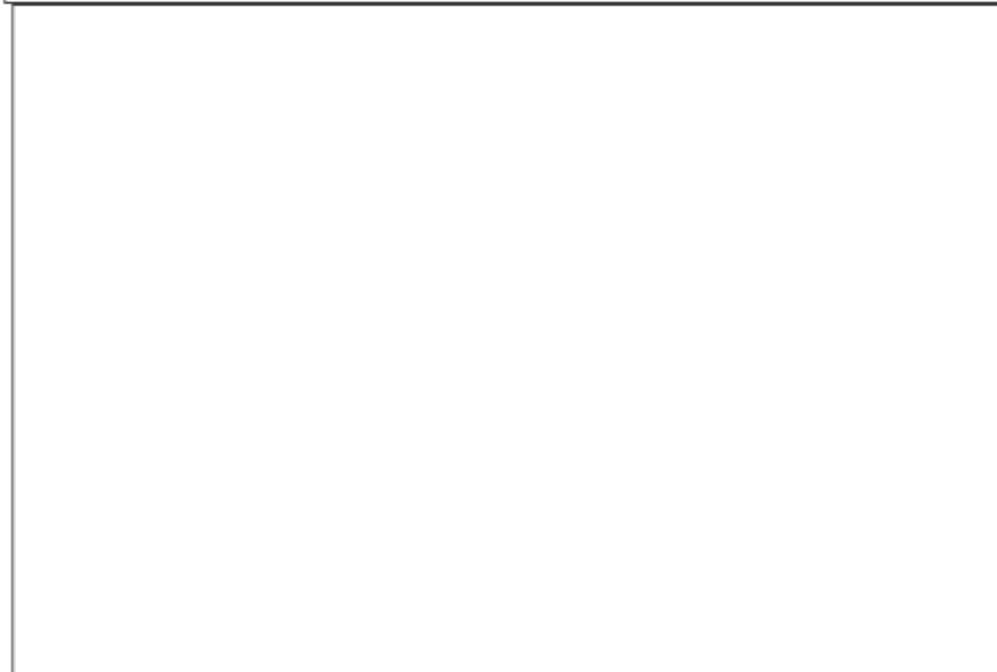
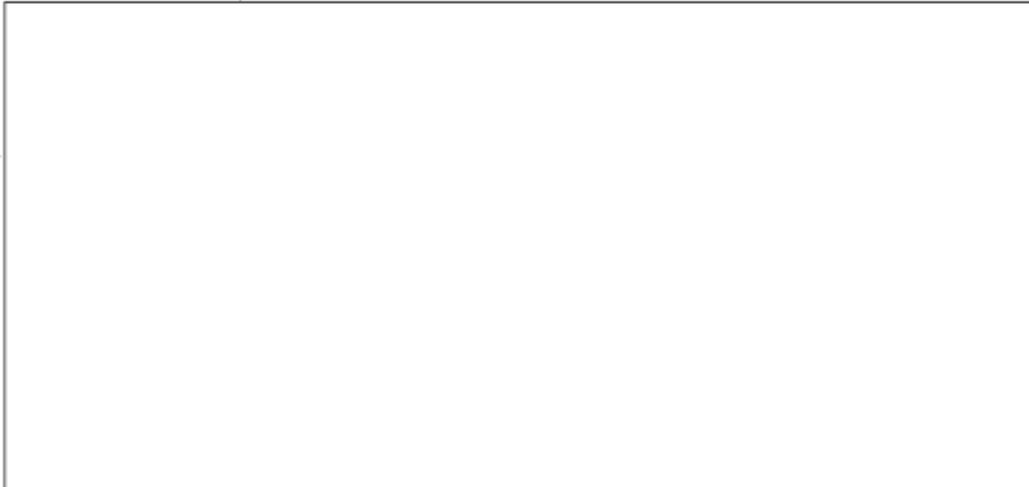
(U) CIA/ORD identified an encryption technology, **digital rights management (DRM)**, to manage usage rights of documents in the classified work environment. DRM technology, developed commercially to manage intellectual property in ebusiness and restrict the copying of CDs, allows the document originator to control user rights to that document at the time it is released. The newest DRM applications, based on the concept of "dynamic DRM," allow the author to enable user controls of a document throughout its life cycle. In dynamic DRM, permissions are controlled at the page level, as a policy server issues encryption keys every time a page is accessed.



3.2 Digital File Management and Control

(U) The S&TWG identified a number of DRM and network audit technologies under evaluation in the classified community. Two pilot programs, discussed below, represent the most advanced applications of these technologies to the unauthorized disclosure problem.





(U) There are challenges to deploying the application in an interagency environment. Currently, its developers are addressing the issue of passing certificates across firewalls at cross-local area network (LAN) connections, as they are attempting to connect the ADSN to the Joint Worldwide Intelligence Communications System (JWICS). A far more daunting challenge to any cross-agency implementation would be integrating the variety and volume of hardware, software, LANs and wide

area networks (WANs), as well as the policies and protocols for handling classified data, found within each organization. The human cost of managing policy rights, page by page, is significant and may be the limiting constraint in the widespread use of DRM.

3.2.2 Auditing Network Activity

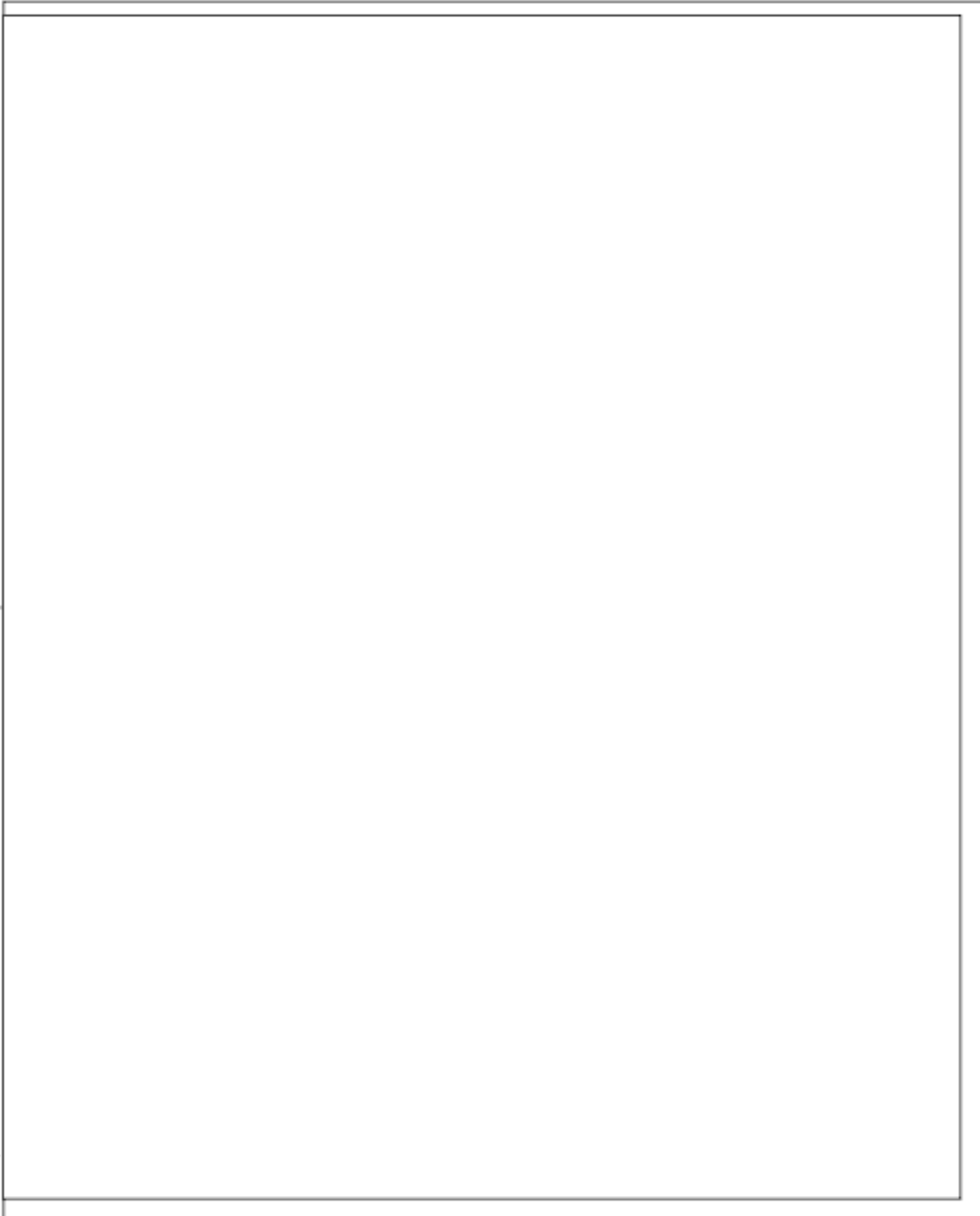
(U) Auditing network and telephone system activity can provide information about whom had access to classified information and when. Obviously it is helpful in forensic analysis after the fact of the leak. It also has the potential to be useful in identifying unusual activities that may be indicative of attempts to gain unauthorized access to classified information. The difficulty in predictive measures is in establishing the criteria for network use that would identify unusual activity.



(U) Features and benefits offered by this application are described in the following table:

~~FOR OFFICIAL USE ONLY~~

DOCUMENT NO. IAFI-UDCI-STG-001
25 MAR 2002



~~FOR OFFICIAL USE ONLY~~

3.3 Paper Document Management and Control

- (U) Portable digital technology may eventually render paper documents obsolete, but this won't happen in the classified environment any time soon. Until it does, organizations must make it much more difficult to copy and walk out of a classified environment with classified documents.
- (U) Tremendous progress can be made in classified paper documentation control by replacing standalone copiers in the classified environment with networked copiers that use scanner/printer technology. DRM technology could then be applied to the units, and only individuals with permission to reproduce hard copy documents will be able to do so. Those without authorization to do so will be stopped, and their attempt will be logged by network audit technology. As an additional, psychological deterrent, biometric identifiers can be added to copiers.
- (U) Still remaining is the issue of enforcing original document controls after printing. Unique identifiers can be included in any printed document to connect a specific copy to the original, controlled information. Paper can be physically tagged, or the classified information itself can be tagged to support internal or criminal investigations of leaks. Here, too, DRM technology can be incorporated with tagging technology to enforce permissions, prevent unauthorized document duplication, and provide tracking data for follow-up investigation.

3.3.1 Watermarks

- (U) Commercially available watermark technology can be used to mark printed documents with a non-removable unique document identifier and visible control statement, e.g., "DO NOT COPY" across the text. Invisible watermarks also can be imbedded into printed information—Xerox and Sharp have copiers that can produce this, and more sophisticated technology is in development. Invisible watermarks can also use technologies that cause very slight moves or shifts of character positions to tag the document. An alternative is to add digital noise pixels to the images or text in the document. Messages like "DO NOT COPY" deliver a behavior deterrent. But more importantly, DRM technology, which can recognize both visible and invisible watermarks, can be used to prevent unauthorized reproduction as documents are scanned and original document rights reestablished.

3.3.2 Word- or Version-Encoding

- (U) Quite possibly, the only potential solution for tracking classified information that leaves the controlled environment through personal conversations or personal notes is to code the information such that the wording, phrasing, or syntax is slightly different in each version-set disseminated. In theory, if the unique words or phrases are found in an unauthorized open source, then investigators can trace them back to those who had access to that particular version. This technique does have its challenges and limitations. There are a finite number of changes that one can make to information without changing the meaning or alerting the reader, and generation of modified versions of classified information is a difficult, manual task. Finally, to be effective, potential leakers must be totally unaware of its use. Thus, word- or version-encoding is applicable to only a small community of interest.

3.3.3 Digital Books

- (U) The use of digital books (also known as electronic books or eBooks) integrated with DRM software could all but eliminate classified information in paper form. Digital books are portable digital data

readers that are used to download and store electronic documents. Access to eBooks could be controlled by any of the electronic authentication techniques available; digital signatures could be included track chain of custody, and they can be tagged so their location is always known. Only downloading would be permitted from authorized secure networks, and these events could be tracked by DRM and audit control applications.

3.3.4 Electronic Document Tags (eTags)

- (U) Physically tagging paper with machine-readable, radio-frequency identification (RFID) tags could be used to prevent the movement of classified paper documents beyond the classified environment. RFID technology is used today in access control systems (e.g., employee badges) and is under consideration for anti-counterfeiting bank notes. eTags respond to an interrogation signal with stored encoded information. By placing interrogation portals at building entrances, Security personnel could be notified when classified documents enter and leave a facility. The technology is potentially useful in small or tightly controlled classified areas, but it may be cost-prohibitive for large-scale use. Current analysis found tags cost from \$1.00 to \$2.00 per page, although they are anticipated to fall to as low as \$.05 per page in the next three years and eventually fall to \$.01 per page as consumer products incorporate the technology.

3.3.5 Compressed-Image File Capture

- (U) Small classified work environments looking to control minor amounts of classified information could implement a system where scanned image files are correlated with stored samples of previously printed documents. Scanned images can be captured as part of an audit process; data storage and size of search space are limitations. Optical character recognition (OCR) software can reduce the data volume of text documents, but it is not effective on non-text documents.

~~(FOUO)~~ A final note on deterrence: to reap maximum "deterrence" benefits from the implementation of technical tools described in this section, their use—and effectiveness—must be publicized to all those with authorized access to classified data.

3.4 Auditing Open Sources

- (U) The S&TWG looked briefly at technologies that could streamline or otherwise improve the labor-intensive open-source reviews most organizations use to uncover leaks of classified information. Data mining, data warehousing, linguistic interpreters, etc., can be used to search open source information for key words or decoy words that identify a leaked source of information. These technologies are currently being developed and used commercially and in the public sector. The S&TWG did not identify any applications within a classified environment but believes several programs do exist in the intelligence community.

3.5 Emerging Technology Threats

- (U) Agencies that handle classified information are always evaluating the potential threat of emerging digital technologies before—and after—they are permitted into the classified environment. Wireless technologies, i.e. cellular phones and wireless LANs, personal digital assistants (PDAs), and other digital-memory tools that satisfy the ever-increasing demand for wider information dissemination and collaboration are but a few technologies that will create holes in existing and proposed classified information control systems. Small, concealable digital cameras with large storage capacities can

quickly image the pages of a large document as they are displayed on the new flat panel computer screens. Commercially available power-line transmission systems used in LANs can be used to exfiltrate digital data.

(U) In its discussions, the S&TWG addressed the potential impact of emerging technologies on existing and proposed systems to prevent the unauthorized disclosure of classified data. At this time, the Working Group offers the following observations and concludes that each of the technologies identified below, as well as all future new technologies, must be fully assessed before they are permitted into the classified environment. Moreover, most emerging digital devices must not be allowed to physically connect to a classified LAN. (LAN access must be managed by a trusted, competent staff.)

- (U) Wireless LANs must be set up properly, with adequate encryption and firewalls, if used to disseminate classified information.



- (U) All power lines in classified facilities must be filtered to defeat attempts to exfiltrate information, especially by use of commercial powerline LAN products.
- (U) Digital cameras should be banned from the classified environment.

4.0 CONCLUSIONS

(U) Specific conclusions of the S&TWG include:

- 4.1 (U) **There is no scientific or technical system or systems that can unequivocally prevent the dissemination of classified information from someone cleared to have it to someone without "need to know."**

(U) There is no scientific or technical solution to prevent the willful disclosure of classified information by someone with authorized access. But technology can close the gaps that allow leaks to occur, leaving only verbal conversations and personal notes as viable means to move classified information out of the classified environment

- 4.2 (U) **Commercially available Digital Rights Management (DRM) technology can provide effective control of classified information on a classified network.**

(U) It is possible to establish positive, persistent control of classified information in hard and soft copy formats with technology discussed in this report, i.e., Documents Rights Management (DRM), audit tools, visible and invisible watermarks, public key infrastructure, centralized server networks with policy servers, and others. Pilots are addressing implementation issues with firewalls and key distribution. Significant issues remain to establishing community-wide policies, standardization of networks and software, and costs and labor of integrating large, distributed user groups.

- 4.3 (U) **Commercially available tools for auditing network and telecommunications activity can be implemented within a classified environment to flag unauthorized activity and, when necessary, support after-the-fact investigation of unauthorized disclosure.**

(U) A comprehensive audit system is only as good as its ability to flag unauthorized use and identify and track access to leaked information. Selecting "events" to audit and designing search algorithms are not trivial tasks, due to the magnitude of information in a large user population.

- 4.4 (U) **The ability to photocopy documents for unauthorized distribution can be substantially reduced by replacing stand-alone copiers with networked copiers, which allow the network to audit activity, take control of a document, and prevent its unauthorized duplication.**

(U) As long as paper and copiers exist in the classified environment, classified documents can be copied and distributed. Changes can be made to the current document copy process to provide more comprehensive audits.

- 4.5 (U) **Wireless technologies, digital cameras, personal digital assistants and other emerging technologies must be carefully assessed before they are permitted into the classified workplace.**

**APPENDIX A:
REFERENCE DOCUMENTS**

Number	Title	Rev.	Date	Source
IPO 00-030	Document Security Program		28 July 2000	CIA/DST/IPO
	Document Copy Study		1995	CIA/DST/ORD
	Document Copy Prevention Requirement Validation Study		1996	CIA/DST/ORD
	Statement of James L. Pavitt, Deputy Director of Operations of the CIA before the SSCI		01 August 2001	Senate Select Committee on Intelligence (SSCI)
	Statement for the Record SSCI Hearing on Unauthorized Disclosures: Supporting Testimony by the Director of CIA		24 May 2000	Senate Select Committee on Intelligence (SSCI)

