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
# 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 .................................................................................................................................. 8  
3.2.2 Auditing Network Activity ................................................................................................ 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  

FOR OFFICIAL USE ONLY
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**

(PQ) 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
2.2 Unauthorized Disclosure Investigation
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) 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:
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 may 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.

(FOLIO) 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

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

VIA: Office of General Counsel

FROM: Vice Chairman, FDDC

SUBJECT: Personal Views on the Inadequacy of Existing Laws Concerning Unauthorized Disclosures, and Recommendations for New Ones

REFERENCE: Leaks: How Unauthorized Media Disclosures of US Classified Intelligence Damage Sources and Methods

This note is intended to supplement the recent paper produced by the Foreign Denial and Deception Committee on leaks. It aims to address implications for legal reforms implied by the findings of that study. The thesis is straightforward: New laws addressing leaks of classified intelligence are urgently needed.

There is a lot of classified information in the press these days, but this note, like the paper, is only concerned with classified intelligence information. Even more narrowly, its focus is confined to intelligence sources and methods, namely, how intelligence is secretly collected and analyzed.

Lessons From the Past: Doing business-as-usual is a prescription for failure

Do we need new laws to address the issue of unauthorized disclosures of classified intelligence information in the media? Answering this question requires some appreciation for the past experience of consistent failure. To date, the most authoritative study addressing unauthorized disclosures is the 1982 “Willard Report” (after its chairman Richard K. Willard, Deputy Assistant Attorney General, Report of the Interdepartmental Group on Unauthorized Disclosures of Classified Information, 31 March, 1982, prepared for the President). It concludes:

“In summary, past experience with leak investigations has been largely unsuccessful and uniformly frustrating for all concerned . . . This whole system has been so ineffectual as to perpetuate the notion that the government can do nothing to stop the leaks.” (Emphasis added).
SUBJECT: Personal Views on the Inadequacy of Existing Laws Concerning Unauthorized Disclosures, and Recommendations for New Ones

The recommendations of the Willard Report for legal correctives resulted in proposed legislation in 1984. Although supported by OMB and the Administration, the Intelligence Community later withdrew the recommended draft legislation due to a perceived lack of support.

Twelve years later, responding to a request from the Assistant to the President for National Security Affairs, the National Counterintelligence Policy Board completed another study and reported no discernible change. (Report to the NSC on Unauthorized Media Leak Disclosures, March 1996). The report explained the continuing failure as a result of two key factors:

- "A lack of political will to deal firmly and consistently with unauthorized executive branch and Congressional leakers. Unsuccessful government efforts to prevent unauthorized disclosures were attributed largely to a lack of political support.

- The use of unauthorized disclosures as a vehicle to influence policy. [Citing the 1987 Tower Commission Iran/Contra report]: 'Selective leaking has evolved to the point that it is a principal means of waging bureaucratic warfare and a primary tool in the process of policy formulation and development in Washington'." (Emphasis in the original)

Given the palpable history of failure in protecting classified intelligence information from press disclosures—and given their epidemic proportions and the deleterious consequences they wreak in countermeasures to US collection effectiveness—it is fair to question whether past failed approaches will work today.

There has never been a general criminal penalty for the unauthorized disclosure of classified intelligence information to the press. Although intelligence leaks can technically be prosecuted under espionage statutes (18 USC 793 and 798), only a single case ever has (US v. Morison, 1988). Given that literally thousands of press leaks have occurred in recent years—many serious and virtually all without penalty—it is clear that current laws do not provide an effective deterrent to leakers or to journalists and their media outlets that knowingly publish classified intelligence.

A new approach—breaking from the failed past. If current trends in unauthorized disclosures are not reversed, such leaks will continue to compromise key sources and methods, and thereby seriously constrain US intelligence capabilities for the present and the future. Since so much now depends on a viable approach to the legal issues that have hamstrung past actions to address this debilitating problem, we need to understand some myths that have impeded past actions.

Popular Legal Myths about Unauthorized Disclosures of Intelligence

1. The current laws are adequate. Despite countless—literally thousands—of intelligence leaks in recent years, only a single violator (Morison, 1988) has ever been prosecuted. Willard's harsh judgment in 1982 that "the whole system is so ineffectual as to perpetuate the notion that the government can do nothing to stop leaks" is even more true today than when he wrote it. Morison notwithstanding, the 20 intervening years have seen neither a discernible abatement in
leaks, nor an improvement in governmental enforcement on this issue. If anything, the problem is getting worse.

Why is this the case? The obvious answer is that the laws are only marginally applicable to leaks, and, as a practical matter, unenforceable in this application. The statute under which Morison was prosecuted (18 USC 793) applies directly to espionage, but presents a real stretch for press leaks; and Morison sold the information to Jane’s Defence Weekly. All agree that the government has always lacked the investigative ability to identify government leakers—and, as the National Counterintelligence Policy Board Study notes, also lacks the political will to bring any case forward. Such a case risks media cries of “chilling effect’ on press discussions, and perhaps would even engender fear among federal employees. However, for press leaks, these laws are irrelevant. Defenders of the legal status quo need to explain the chasm between damaging leaks and the crippling lack of enforcement—and how present laws can successfully address this issue now when they never have before. I think they cannot even make a plausible argument in the face of the evidence at hand.

The lack of enforcement is itself the best indicator of the deficiencies in the law. Current law provides no appreciable deterrent to leakers or to their press publicists. Some journalists even demonstrate contempt for the law, and mock the government’s inability to control leaks:

“We believe in stories that make you say ‘holy shit’ when you read them, said Bill Gertz of The Washington Times, in a flattering profile of him that appeared in the conservative Weekly Standard . . . Over the past couple of years, Mr. Gertz has written more stories based on classified government documents than you can shake a stick at, infuriating Clinton Administration officials and making a mockery of official classification policy.” (Steven Aftergood, in Secrecy in Government Bulletin, No. 64, Jan., 1997, p. 1).

Mockery is correct. Journalists who traffic in classified information can proceed with high confidence that they can publish this information at will, and do so without penalty; and their government suppliers seem not to be deterred either. Laws that invite mockery because they are so ineffectual have lost whatever usefulness they might have had. Worse, they are positively counterproductive: They leave the impression of their adequacy while keeping government legally paralyzed to stem the hemorrhage of classified sources and methods appearing with alarming frequency in the US media.

2. Leaks really don’t do much harm. The genealogy of this view traces to the publication of the Pentagon Papers. After much government carping about all the damage that those Top Secret revelations in the press would do to US national security, few today would claim that any damage was done at all. And certainly none to intelligence sources and methods. This view is given even greater credence by another popular myth that the government over-classifies everything, and classifies way too much. This seduction has become a creed among anti-secrecy proponents such as the National Security Archive and Federation of American Scientists. Publicly, this view is accepted uncritically, and never contested. Nor refuted. In fact, as the recent FDDC classified study of media leaks has convincingly shown, leaks do cause a great deal
of harm to intelligence effectiveness against priority issues including terrorism. But intelligence professionals also appreciate, and are much frustrated by, the fact that the best arguments for stopping intelligence leaks simply cannot be made in the press or in public forums, because of the paradoxical need to discuss—but protect—classified information.

3. **Intelligence is adequately protected as “national defense information.”** This myth highlights the added legal difficulties of showing that intelligence sources and methods need also to be proven as “national defense” information to warrant protection under 18 USC 793, 798, and related laws. In truth, intelligence may or may not be so defined, but often, intelligence issues do not pertain directly to the national defense, and the added legal burden of meeting this defense requirement imposes still another pointless obstacle to legal remedies. Presently, the burden of proof is on the government to show that intelligence information relates directly to national defense, and further, that the person compromising it knew beforehand that its disclosure could harm the national defense. This burden is too high and off the mark. What intelligence information needs is a separate, discrete, legal identification, independently of national defense. This would create a legally-protected category of intelligence information that does not now exist. Other categories that are afforded effective protection include information on banking, crop estimates, taxes, and consumer credit. Surely intelligence sources and methods deserve as much. Sources and methods of intelligence collection are intrinsically important to the Nation’s security, and intrinsically worthy of separate statutory protection. In removing impediments, this distinction would thus provide a major step forward in making enforcement—investigation and punishment—easier.

4. **Public trials for secret issues are necessary.** This bedeviling limitation has hamstrung the government in prosecuting espionage cases—and serves as a major inhibitor even in cases of unauthorized disclosures in the media. (It also provides a compelling rationale for military tribunals for terrorist cases involving foreign nationals). While the Classified Information Procedures Act (CIPA) affords good protection in pre-trial protection and “in camera” procedures, the perennial risk of exposing sensitive information in open court proceedings often deters the government from taking action. For example, an investigation of a major disclosure of highly classified information about sensitive collection activities might never be started—or could soon be halted—due to acute worries over further revelations about sources and methods. The reason? Intelligence agencies justifiably fear additional exposures of even more sensitive information in legal proceedings that would follow. As a result, significant leaks investigations always face the risk of being aborted after start-up, or are not started at all. This extraordinary Catch-22 is that the greater the sensitivity—and intrinsic importance to national security—of the information compromised in the media, the greater the incentive for governmental inaction. Poor laws that cannot adequately safeguard classified intelligence information in judicial proceedings guarantee continued governmental inaction—and continued media compromises of uniquely valuable sources and methods without penalty.

5. **Journalists have every right to publish classified information.** I do not understand how this myth got started, and it certainly doesn’t apply to all journalists. But it applies to some. Unhappily, professional journalists must count within their ranks a few colleagues who traffic
heavily in classified intelligence—high volume, and often highly classified. When this minority of journalists arrogate to themselves the presumptive right to publish classified information in US newspapers and books, and on the Internet, it is fair to ask where they got this right. US classified information is produced by fully lawful procedures in the Executive Branch, and is subject to oversight by the Legislative Branch. No authorization to overturn this system extends to the Fourth Estate. But some journalists presume this “right” and exercise it presumptively on behalf of the American people—much to the detriment of the population they claim to serve when intelligence capabilities are weakened as a result.

These journalists either assume that existing law doesn’t apply to them, or if it does that it won’t be enforced, or that they are not breaking any laws at all. A few arrogant journalists—whose incomes and careers benefit from exploiting classified intelligence for profit—treat legally-classified intelligence as if it didn’t deserve any protection at all. But their unquestioned legal right to do this has yet to be established in law. In practice, their actions subvert lawful regulations that fully intend to protect the intelligence they compromise in the press. In publishing classified intelligence, no journalist can convincingly claim a constitutional right to do so. Any journalist’s “right” to publish information should not extend to classified information. But this legal argument remains to be made or adjudicated.

6. First Amendment protections prevent more restrictive legislation. For the most part, this is a canard. Identifying and punishing government leakers should not invite constitutional apprehensions. Leaking classified intelligence is no one’s legal right, and publishing it in the press has not been demonstrated as the media’s constitutionally-protected right either.

Still, the inherent tension between First Amendment rights and the government’s interest in protecting national security is dynamic, and may never be solved “once and for all.” But the current balance so favors First Amendment rights that legitimate national security interests are often superseded. This seems certainly the case with unauthorized media disclosures that compromise intelligence effectiveness. Here we should entertain redressing a potential legal imbalance by reconsidering a time-tested democratic principle enunciated by the preeminent philosopher of liberty, John Stuart Mill:

“... the only purpose for which power can rightfully be exercised over any member of a civilized community, against his will, is to prevent harm to others.” On Liberty (1859).

Under the “harm principle”—for example, yelling “FIRE!” in a theater when there is none—a variety of exceptions to free speech are well established in American law such as obscenity, defamation, breach of peace, “fighting words,” and sedition. To this list we should add the compromise of US intelligence sources and methods required in the service of the Nation’s security. Government leakers with authorized access to the classified information they pass to journalists, and—certainly in egregious cases, also the journalists who traffic in classified intelligence—should be legally accountable for the sources and methods they expose that will
help foreign adversaries degrade the effectiveness of US intelligence, and thereby, further jeopardize US national security. By “egregious” I mean:

- When a covert intelligence officer or a foreign agent’s identity is compromised in the media, thus risking exposure that may end in imprisonment or death.

- When multiple sources of fragile collection, including technical sensors, are compromised in the media, thereby incurring reduced effectiveness—for example, against priority targets such as Usama Bin Ladin or al-Qai’da—enfeebling analysis or warning through weakened collection.

- When extremely sensitive, highly classified, and costly collection programs are compromised in the media, resulting in foreign countermeasures that significantly reduce the program’s cost-effectiveness.

- When unauthorized disclosures have so impaired intelligence on key national issues such as terrorism or proliferation of weapons of mass destruction that US policymakers are deprived of valuable information—including intelligence warning—not otherwise available, but essential to sound decisions and policies affecting US national security.

Attributes of a Good Law

The scope and seriousness of the intelligence leaks problem argue strongly for urgent attention to new law that can successfully stem the hemorrhage of classified intelligence that regularly appears in the media. We need a specific statute that will deter leaks, and that will punish those who compromise classified intelligence that helps foreign adversaries defeat US sources and methods. What attributes should such a law have? It should:

- Unambiguously criminalize unauthorized disclosures of classified intelligence information.

- Hold government leakers accountable for providing classified intelligence to persons who are not authorized access to that information.

- Define intelligence information—and specifically sources and methods—distinctly from defense information, creating a protected category of information less vulnerable to exposure under First Amendment rights.

- Provide better protection to sensitive and classified intelligence information in court trials and other judicial proceedings than is presently afforded through CIPA.

Should journalists have accountability? Much or all of the above attributes can be accomplished without inviting serious debate over First Amendment issues. More controversially, such a law would also hold uncleared publicists—i.e., journalists, writers,
publishing companies, media networks, and websites who traffic in classified information—accountable for damaging disclosures. Specifically, media should be held responsible for providing mass publicity to significant intelligence information they know to be classified, and whose exposure reduces US intelligence effectiveness by damaging sources and methods.

Present law already establishes such liability for media representatives who compromise the covered identities of US intelligence officers and agents (50 USC 421-426—but only as a pattern of activities, not for a compromise that could or does lead to the imprisonment or death of an agent caused by a single article); and also for compromises of SIGINT information (18 USC 798). Under these statutes—which have never been enforced against cases of unauthorized disclosures—compromises of imagery and other technical intelligence are not covered. And no generalized provision exists that will impose penalties for the publication of intelligence information that leads to foreign countermeasures that degrade, neutralize, or deceive US sources and methods of sensitive intelligence collection programs.

Consequences of inaction. Unless comprehensive measures are taken to identify and hold leakers accountable for the significant, often irreversible, damage they inflict on vital US intelligence capabilities, and, by implication, the degraded support such weakened intelligence offers to policymakers and warfighters, the damage will continue unabated. Conceivably, without some legally effective corrective action, the situation could even worsen. Under this scenario:

- Policymakers, warfighters, and military planners should expect that their intelligence on significant national security issues will be less accurate, complete, or timely than it would be without foreign countermeasures made possible by unauthorized disclosures.

- American citizens should expect that timely warning of surprise attacks against the United States by terrorists or other hostile adversaries will be degraded because key collection activities have been rendered less effective through unbridled leaks.

- US taxpayers should expect that their multi-billion dollar collection programs will be less cost-effective than they would otherwise be if foreign adversaries were not learning how to neutralize such programs through extensive classified information readily available in open sources.

The alternative is better intelligence capabilities for the United States. This can result from no added costs by merely better protecting the sources and methods we now have and those that are in the pipeline. Stemming press leaks will afford significantly better protection. Better laws—and enforcement of these laws—will make this possible. Present laws preclude improvement.
Inter-Agency Task Force on Unauthorized Disclosures
Security Working Group

Tasking: The Interagency Task Force (IATF) on Unauthorized Disclosures Security Working Group was tasked with taking a fresh look at ways to organize and structure a more effective and comprehensive approach to addressing and minimizing the problem of unauthorized disclosures (leaks) of US classified intelligence information to the media. The purpose of this report is to provide the IATF with a brief overview of the Security Working Group’s (SWG) progress to date.

Challenges

Number of Potential Suspects: The SWG members believe that measures to reduce the number of possible leak suspects would greatly assist in the task of identifying and sanctioning leakers. Even in cases in which highly sensitive restricted program information is leaked, investigators typically find that there are literally hundreds, if not thousands of individuals who had access to the compromised information. It is estimated that Intellink alone, has approximately 100,000 users. Today, increased collaboration requires even broader dissemination of classified information. The challenge, therefore, is identifying and deploying technical tools that will enhance the leaks investigator’s ability to narrow the field of potential suspects.

Unified Effort: Another key area identified by the group is the need for a unified government-wide program to identify, analyze, and investigate media leaks and report investigative findings to appropriate officials for administrative or criminal sanctions. Currently, the various agencies of the Intelligence Community (IC) have their own agency-specific unauthorized disclosure programs. On virtually every media-leak related issue discussed, to include investigative tools, processes and policies, the group found little uniformity. For a variety of reasons, many organizations lack formal dedicated media leak investigation programs. With some exceptions, in the past 10 years, the only individuals who have been identified and administratively sanctioned for leaking classified information to the media were those who self-confessed or were identified by the media as the source of the leaked information. The group believes that a more unified IC, OGA, and Industry wide program, including establishment of leak detection units in each agency and a community-wide leaks investigation unit, would significantly enhance the identification, authentication, investigation and prosecution of media leaks.
Lessons Learned

Past attempts to coordinate the Community have met with only sporadic and minimal results. The DCI's Unauthorized Disclosure Analysis Center (1986-1992) (UDAC) incorporated some Intelligence Community participation and an analytical arm, but lacked investigative and education capabilities. As a result, media leak analysis and leak investigations were almost totally disconnected and uncoordinated.

Recommendation:
UNCLASSIFIED FACSIMILE TRANSMITTAL FORM

DATE: 02/19/2002

SENDING FAX TELEPHONE NUMBER: 

RECEIVING FAX TELEPHONE NUMBER: [______] opr 62

NUMBER OF PAGES 3 (Including Transmittal Form)

FROM: Office of Security/CIA

(SUBJECT: Minutes from the Security Working Group meeting 02/14/2002)

TO: (ADDRESSEE/ORGANIZATION/OFFICE/EXTENSION)

1. James Duncan DoJ/OPR [______] opr 62

2. 

3. 

4. 

5. 

6. 

7. 

8. 

9. 

10. 

SPECIAL INSTRUCTIONS: The Working Group meeting for Thursday, 2/21 is canceled. The next meeting will take place on Thursday, 2/28 (same time, same place).

RELEASING OFFICIAL: (PRINTED NAME) (SIGNATURE)

RECEIVING STATION USE ONLY

Please receipt for material by entering time of receipt/signature and transmit back to sending station.

DATE/TIME: SIGNATURE:

FORM 10-92 4383 (EF)

APPROVED FOR RELEASE
DATE: DEC 2006
Inter-Agency Task Force on Unauthorized Disclosures
Security Working Group Meeting Minutes
Central Intelligence Agency

Thursday, 14 February, 2002
1:00-2:30 p.m.

ATTENDEES:
Jeff Gaynor, Co-Chair, OSD/OASD
Bernadine Ayer, OSD/OASD
NIMA/Legal
NIMA
NSA
CIA/OGC
Nancy Rolph-O'Donnell, DoS/DSS
Richard Ingram, DoS/DSS
CIA/OS
Betsy York, FBI
DIA
James Duncan, DoJ/OPR
CIA/OS
NRO

James Duncan updated the group on the Litigation Group's progress. Their recommendations to the IATF will be finalized this week and some of their recommendations will more than likely overlap with the Security Working Group's recommendations.

informed the group that (CIA) has been tasked by CIA/OGC to prepare a document regarding damage assessments in regard to media leaks. Two versions will be prepared; one unclassified and one classified.

The following questions (received from the 02/12/2002 IATF meeting) were discussed:

- What processes/procedures exist for revocations? How many steps/reviews are required before a decision is rendered?
  - Should our processes be consistent across all organizations?
What, if any, changes would we advocate?

- What procedures exist to protect whistleblowers? Are these protections adequately communicated to the employees?

Each member gave a brief overview of their agency's processes/procedures for security revocations. It was the consensus of the Working Group that security revocation procedures should be consistent throughout the Intelligence Community. The Group also discussed the need for publication of adverse actions against employees for unauthorized disclosures throughout the Intelligence Community as a means of deterring future unauthorized disclosures.

With regard to whistleblowing, members agreed that their respective agencies have ample resources allocated to educate employees on procedures and protections.

Also addressed was whether or not EO 12968 should be revised. Most members agreed it should not be revised, however, the NIMA and DoD Working Group members thought otherwise. The processes employed by their agencies is much more cumbersome than the other agencies represented.

**Tasking #1:** review the Interim Report from the Legislative Working Group and bring comments to the next meeting.

**Tasking #2:** allow others within your respective organizations to review the Security Working Group Status Report and bring any questions/concerns to the next meeting.
SECURITY WORKING GROUP ISSUES

1. What sanctions have been imposed on government employees in the past 5-10 years for leaks; for mishandling classified information?

2. Warrantless Searches of US Government offices:
   - DOJ policy imposed government-wide
   - Adverse inference in Administration Proceeding

3. Single Issue Polygraphs:
   - Adverse Inference in Administration Proceeding

4. Refusal to answer questions or be interviewed:
   - Adverse inference in Administrative proceeding

5. DCI is statutorily required to protect sources and methods of intelligence:
   - Is he applying adequate resources to this endeavor?

6. Traps and traces on government phones:
   - cost
   - feasibility

7. Develop educational programs:
   - What programs are currently in place?
   - remark on their efficacy utility