Office of the Attorney General
Washington, D.C. 20530

October 15, 2002

The Honorable J. Dennis Hastert
Speaker of the House of Representatives
U.S. House of Representatives
Washington, D. C. 20515

Dear Mr. Speaker:

The President and I place deterring, detecting, and punishing unauthorized disclosures of U.S. national security secrets among our highest priorities, at all times, but especially in this time of war against terrorism of global reach. There is no doubt and ample evidence that unauthorized disclosures of classified information cause enormous and irreparable harm to the Nation's diplomatic, military, and intelligence capabilities. They impair, especially, the Intelligence Community's ability to provide essential support to U.S. national security policymakers and our military's ability to provide for the national defense. We need an effective Government-wide program to curtail these damaging disclosures and to hold the persons who engage in unauthorized disclosures of classified information fully accountable for the serious damage they cause to intelligence sources and methods, military operations, and to the nation. Those who would break faith with the American people and disclose classified information without authority to do so will face severe consequences under the law.

Section 310 of the "Intelligence Authorization Act for Fiscal Year 2002" (Public Law 107-108, December 28, 2001) provided that:

> . . . The Attorney General shall, in consultation with the Secretary of Defense, Secretary of State, Secretary of Energy, Director of Central Intelligence, and heads of such other departments, agencies, and entities of the United States Government as the Attorney General considers appropriate, carry out a comprehensive review of current protections against the unauthorized disclosure of classified information . . . .

Section 310 called for a report from the Attorney General to Congress containing a comprehensive description of the review, including the Attorney General's findings, an assessment of the efficacy and adequacy of current laws and regulations against the unauthorized disclosure of classified information, and any recommendations for legislative or administrative action that the Attorney General considers appropriate.

To assist me in implementing Section 310, I formed an interagency task force, including representatives of those with whom the statute asked me to consult, to review the subjects addressed in Section 310 and to provide information and advice to me. I have reached my findings, made my assessments, and formulated my recommendation, which are reflected in this report to Congress under Section 310.

FINDINGS AND ASSESSMENT

The President has the power under the Constitution to protect national security secrets from unauthorized disclosure. This extends to defining what information constitutes a national security secret and to determining who may have access to that secret. In *Department of the Navy v. Egan*, 484 U.S. 518, 527 (1988), the Supreme Court made these points clear:

The President, after all, is the "Commander in Chief of the Army and Navy of the United States." U.S. Const., Art. II, § 2. His authority to classify and control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position in the Executive Branch that will give that person access to such information flows primarily from this constitutional investment of power in the President and exists quite apart from any explicit congressional grant. See *Cafeteria Workers v. McElroy*, 367 U.S. 886, 890, 81 S. Ct. 1743, 1746, 6 L. Ed. 2d 1230 (1961). This Court has recognized the Government's "compelling interest" in withholding national security information from unauthorized persons in the course of executive business. *Snepp v. United States*, 444 U.S. 507, 509, n. 3, 100 S. Ct. 763, 765, n. 3, 62 L. Ed. 2d 704 (1980). See also *United States v. Robel*, 389 U.S. 258, 267, 88 S. Ct. 419, 425, 19 L. Ed. 2d 508 (1967); *United States v. Reynolds*, 345 U.S. 1, 10, 73 S. Ct. 528, 533, 97 L.Ed. 727 (1953); *Totten v. United States*, 92 U.S. (2 Otto) 105, 106, 23 L. Ed. 605 (1876). The authority to protect such information falls on the President as head of the Executive Branch and as Commander in Chief.

Presidents have exercised by Executive Order their constitutional authority to establish systems for determining what constitutes a national security secret and who may have access to such secrets. Currently, the determination of what constitutes a national security secret is governed by Executive Order 12,958 of April 17, 1995, as amended and the determination of who may have access to such secrets is governed by Executive Order 12,968 of August 2, 1995, as well as by Executive Order 12,958.

The laws of the United States assist in implementing the President's constitutional powers. Laws providing for disclosure of government information exempt national security secrets from disclosure. *See*, for example, Freedom of Information Act (FOIA) (5 U.S.C. §552(b)(1)); Government in the Sunshine Act (5 U.S.C. §552b (c)(1)); Privacy Act (5 U.S.C. §552a(k)(1)); Federal Advisory Committee Act (5 U.S.C. Appx. II); Administrative Procedures Act (5 U.S.C. §553); National Environmental Policy Act (42 U.S.C. §4332(2)(C)); and Paperwork Reduction Act (44 U.S.C. §3501, *et seq.*). Federal law also makes certain disclosures of specified national security secrets a crime. *See*, for example, statutes prohibiting disclosures

of national defense information, intercepted communications or codes (18 U.S.C. §§793, 794, 797, 798 and 952); statute prohibiting the unauthorized disclosure of restricted data (42 U.S.C. §2277); the Intelligence Identities Protection Act (50 U.S.C. §421 *et seq.*); and Internal Security Act (50 U.S.C. §783).

Although there is no single statute that provides criminal penalties for all types of unauthorized disclosures of classified information, unauthorized disclosures of classified information fall within the scope of various current statutory criminal prohibitions. *See United States v. Morison*, 844 F.2d 1057 (4th Cir. 1988). It must be acknowledged that there is no comprehensive statute that provides criminal penalties for the unauthorized disclosure of classified information irrespective of the type of information or recipient involved. Given the nature of unauthorized disclosures of classified information that have occurred, however, I conclude that current statutes provide a legal basis to prosecute those who engage in unauthorized disclosures, if they can be identified. It may be that carefully drafted legislation specifically tailored to unauthorized disclosures of classified information generally, rather than to espionage, could enhance our investigative efforts. The extent to which such a provision would yield any practical additional benefits to the government in terms of improving our ability to identify those who engage in unauthorized disclosures of classified information or deterring such activity is unclear, however.

Regardless, the vital need in protecting national security secrets must include rigorous investigation of unauthorized disclosures of classified information to identify the individuals who commit them, and vigorous enforcement of the applicable administrative, civil, and criminal provisions already available.

With respect to administrative actions to address unauthorized disclosures of classified information, information security programs across Government are fragmentary. A comprehensive, coordinated, Government-wide, aggressive, properly resourced, and sustained effort to address administratively the problem of unauthorized disclosures is a necessity. Departments and agencies should use all appropriate investigative tools and techniques at their disposal to identify those who commit unauthorized disclosures of classified information. Immediate and consequential administrative investigations that are coordinated across agencies responsible for handling classified information would provide a large measure of deterrence. An active and aggressive administrative approach to the problem of unauthorized disclosures by all departments and agencies could result in additional criminal prosecutions.

The responsibility for correcting the problem of unauthorized disclosures of classified information falls squarely upon the shoulders of all Government officers and employees who are privileged to handle classified Government information. Department and agency heads have substantial authority to address the problem of persons who engage in the unauthorized disclosure of classified information within their own organizations through suspension or revocation of clearances and procedures to terminate employees in the national security interests of the United States. They have limited authorities with respect to unauthorized disclosures

outside their own organizations. In most of the few cases in which a person who engaged in an unauthorized disclosure of classified information has been identified, the sanctions applied have been relatively inconsequential in comparison to the damage caused as a result of the unauthorized disclosure. In most cases, identifying the individual who disclosed classified information without authority has been difficult, at best.

The risks of unauthorized disclosures of classified information associated with the large numbers of people with access to such classified information must be managed intelligently, appropriately, and effectively. Managing this risk requires strict enforcement of the principle that no individual should have access to a particular national security secret unless the person has the requisite security clearance and access approval and needs to know the secret to perform the individual's official duties. Discipline with respect to the extent of dissemination of particular classified information will help reduce the opportunities for faithless individuals to engage in unauthorized disclosure of classified information, and will underscore for individuals who have the privilege of access to classified information that they have personal accountability and legal liability for the protection of the information.

Technological applications, within a reinvigorated information security regime, may be able to substantially improve the management and control of classified information. However, we cannot rely on technology alone. Without renewed emphasis on personnel, communications, and information security, technology by itself cannot be expected to reduce substantially the occurrence of unauthorized disclosures of classified information. Technology, if embraced and applied intelligently, can provide a strong deterrent, detection, and forensic capability in combating unauthorized disclosures. Technology can provide the investigators, the administrators, and potentially the prosecutors, with better tools to identify and punish those responsible for violating their legal and ethical obligations to protect classified information. Commercially available digital rights management technology holds substantial promise in providing effective control of the integrity of classified information. Digital rights management technology was developed by the private sector to manage intellectual property in e-business and to restrict the copying of compact discs. Commercially available tools for auditing network activity also can be applied within the classified environment to identify unauthorized activities, particularly with respect to post-disclosure forensic investigative support. If technology is not embraced and mastered to protect information, and to deter and detect its misuse, we will be significantly hampered in our ability to address adequately the problem of unauthorized disclosures.

The seriousness of the issue has outpaced the capacity of extant administrative and law enforcement mechanisms to address the problem effectively. I therefore recommend that the U.S. Government attack the problem of unauthorized disclosures of classified information simultaneously on three fronts.

RECOMMENDATIONS

First, the Executive Branch must activate a wide range of administrative measures to significantly improve our capacity to stem the practice of unauthorized disclosures of classified information.

Second, all departments and agencies that originate or handle classified information must take aggressive steps and use all appropriate means at their disposal – individually and collectively – to identify and impose sanctions on those who reveal classified information without authority.

Third, policy and legal officials in the Departments of Defense and Justice, and the Director of Central Intelligence (DCI) for the Intelligence Community, must work together to improve enforcement of existing laws. Likewise, these officials must work closely with Congress to ensure that we have the necessary legal authorities to enhance our ability to deter such unauthorized disclosures and to identify and hold accountable those who, without authority, reveal classified information, both for violations of their duty to the United States and for any violations of law. Until those who, without authority, reveal classified information are deterred by the real prospect of productive investigations and strict application of appropriate penalties, they will have no reason to stop their harmful actions.

Thus, specifically, I recommend that:

- Departments and agencies that originate, disseminate, or handle classified information should continue to use their authorities to undertake immediate and aggressive investigations of unauthorized disclosures of classified information utilizing all appropriate and available investigative tools and techniques to identify the perpetrators.

- Departments and agencies should continue to report these crimes to the Department of Justice under established reporting requirements, and should not delay their internal investigations pending the Department's prosecutorial decision on the matter, unless the Attorney General directs otherwise in a particular case.

- In conducting their internal investigations, departments and agencies should consult with the FBI for investigatory guidance, but the FBI will not – at the initial stage of the investigation – be the lead investigative agency, unless the Attorney General directs otherwise in a particular case.

- Given the significant harm that results from unauthorized disclosures of classified information and the nature of investigations involving unauthorized disclosures of classified information, the Department of Justice will provide active investigative support to the conduct of these investigations, as directed by the Attorney General.

- Upon the request of the head of a department or agency, and with respect to intelligence information upon the request of the DCI, and as the Attorney General may direct, the FBI and the Criminal Division of the Department of Justice for investigative and prosecutorial purposes, respectively, should devote the necessary resources to pursue unauthorized disclosures of classified information, including taking the lead responsibility for a particular investigation at the appropriate stage.

- The authorities of the Department of Justice, including the FBI, will continue to be available where needed to conduct effective investigations of unauthorized disclosures of classified information.

- Upon identification of a person who engaged in an unauthorized disclosure of classified information, the agency concerned should refer the matter to the Department for a prosecutive decision.

- The Department of Justice will be prepared to prosecute all cases where the evidence and circumstances warrant, and, as appropriate, provide regular status reports to the affected departments or agencies.

- Departments and agencies should promptly notify the Department of Justice when a current or former employee or other person with a contractual or other legal obligation to the Government to protect classified information engages in an unauthorized disclosure, and the Department of Justice should vigorously pursue civil enforcement actions against such individuals.

- Executive Orders 12,333; 12,958; 12,968; and other applicable authorities should be reviewed, and consideration given to enhancing the DCI's authority and responsibility to protect intelligence sources and methods across Government and to enhancing other agencies' authority to protect classified information under their areas of responsibility.

- The Executive Branch should continue to engage Congress, the media, and the American people, to increase awareness of the damage to national security resulting from unauthorized disclosures of classified information and the need to improve the federal government's classified information security practices and enforcement of laws concerning unauthorized disclosures.

- The non-disclosure agreements signed by all persons who are granted access to classified information should be amended to include a provision that sets out liquidated damages, when appropriate, based upon a judicial finding that the person breached that contract by having engaged in an unauthorized disclosure of classified information; and to require that the individual, upon request of a duly authorized official during the course of an unauthorized disclosure investigation, execute a certification under penalty of perjury that he or she has not engaged in a specified unauthorized disclosure of classified

information.

- A comprehensive, coordinated, Government-wide, properly-resourced, and sustainable program must be developed to reemphasize the need for protection of classified information, the substantial harm that results from unauthorized disclosures, and severe penalties that will be imposed in accordance with the law on those found to have engaged in unauthorized disclosures of classified information.

    - This program should emphasize personal accountability and legal liability for the protection of classified information.

    - This program should reemphasize the principle of "need-to-know" with respect to the dissemination of classified information.

    - This program should use all available methodologies for increasing information security awareness, including through e-mails, regularized and non-adversarial defensive briefings at all levels of Government service, Internet postings, and more routine security awareness posters.

- Department and agency heads should review their legal authorities and associated administrative processes to determine their adequacy to investigate and to impose effectively and quickly appropriate sanctions upon someone determined to have engaged in an unauthorized disclosure of classified information.

- The Department of Justice will continue to review its legal authorities, policies, and practices to determine their adequacy to assist in the identification of those who without authorization disclose classified information to others who are not eligible to receive it.

- Department and agency heads, including the Secretary of Defense, the Attorney General, and the DCI for the Intelligence Community, should ensure that organizations within their authority are provided sufficient resources to:

    - strengthen information security programs established pursuant to applicable Executive Orders or statutes;

    - ensure provision of analytical support to security investigators;

    - use cross-agency resources to develop a relational database on unauthorized disclosures of classified information;

- support investigations of unauthorized disclosures of classified information across departments and agencies, to the fullest extent consistent with applicable law;

- promote consistent application of security rules and procedures within organizations under their respective responsibilities, consistent with the guidance provided by the DCI pursuant to applicable Executive Orders; and

- recommend technological applications for information systems that handle classified information.

- Department and agency heads whose organizations originate, disseminate, or handle classified information should remind their employees regularly of department or agency policy regarding who within the department or agency is authorized to initiate or respond to contacts with the news media.

- Technological enhancements to the protection of classified Government information must continue to be developed and implemented.

- Dynamic Digital Rights Management technology and other similar security software applications should receive significant study to determine their particular efficacy in the cross-agency classified environment.

- Technology enhancements should include a more agile and flexible auditing capability to provide investigators with more detailed information about specific sites, the duration of visits, the documents viewed by particular users, and whether copies of documents were produced.

- Software applications should be developed and implemented that can limit access to defined areas of Intelink and any other shared databases containing classified information to those with appropriate clearances and need to know.

The recommendations above for administrative action are within the existing authorities of the Executive Branch and do not require additional legislation. Jointly with the DCI, I plan to discuss steps to implement these recommendations with the Assistant to the President for National Security Affairs, the Secretary of Defense, and other department and agency heads as appropriate. We should continue to explore what additional specific steps are needed to strengthen the ability of the United States Government to combat unauthorized disclosures of classified information, to include continued consideration of various legislative options. It is

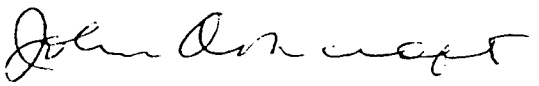
critical that any momentum generated by the Task Force's review and this report brings about concrete improvements in our treatment of this serious problem.

CONCLUSION

In sum, to protect its diplomatic, military, and intelligence capabilities, the Nation must combat unauthorized disclosures of classified information effectively, through aggressive administrative enforcement of current requirements, rigorous investigation of unauthorized disclosures, and vigorous enforcement of the criminal laws that make such disclosures a Federal crime. Clearly, that only a single non-espionage case of an unauthorized disclosure of classified information has been prosecuted in over 50 years provides compelling justification that fundamental improvements are necessary and we must entertain new approaches to deter, identify, and punish those who engage in the practice of unauthorized disclosures of classified information. Although there may be some benefit from a new comprehensive criminal statute, such a statute standing alone would be insufficient in my view to meet the problem of unauthorized disclosures of classified information in its entirety. Accordingly, I am not recommending that the Executive Branch focus its attention on pursuing new legislation at this time. Should Congress choose to pursue a criminal statute that covers in one place all unauthorized disclosures of classified information, however, the Administration would, of course, be prepared to work with Congress.

The Office of Management and Budget advises that there is no objection to the submission of this report from the standpoint of the Administration's program.

Sincerely,



John Ashcroft
Attorney General

cc: The Honorable Dick Cheney
President of the Senate
United States Senate