Department of Justice

STATEMENT OF

ERIC H. HOLDER, JR.
ATTORNEY GENERAL

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

AT A HEARING CONCERNING

UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION

PRESENTED ON

DECEMBER 3, 2009

STATEMENT
OF
ERIC H. HOLDER, JR.
ATTORNEY GENERAL

BEFORE THE
SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

AT A HEARING CONCERNING
UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION

PRESENTED ON
DECEMBER 3, 2009

Madam Chairman, Mr. Vice Chairman, and Members of the Committee, thank you for the opportunity to discuss both the problem of unauthorized disclosures of classified information to the media and the Department of Justice's handling of such matters.

First, the problem: Unauthorized leaks of classified and sensitive information have frustrated many Administrations – Democratic and Republican – for decades. I am not the first Attorney General to come before this Committee to discuss the problem of leaks and to explore possible solutions. The Department of Justice has worked hand in hand with our partners in the Intelligence Community and with the Congress for many years to address this problem. There are no easy solutions or quick fixes.

While this Administration strongly favors transparency, unauthorized leaks of classified and other sensitive information are a real threat to our national security. Leaks allow adversaries of the United States to have access to some of our most sensitive information. They have caused the loss of important and expensive intelligence capabilities and programs, compromised assets, and hindered important government functions. The failure to treat and protect sensitive

information properly is a grievous breach of the public trust that undermines our nation's security.

One common example of the way important government functions are hindered by leaks of sensitive information can be found in the damage they do to our relationships with other governments. Foreign governments regularly share sensitive information with the United States Government to assist us in important matters, such as counterterrorism and counter-proliferation efforts. This information is generally shared with the promise that the information and its source will be protected. If the information is subsequently leaked, it can damage our relationships with governments that are willing to share information with us, and deter future cooperation that is imperative in the fight against terrorism and weapons proliferation.

Now let me turn to the Department's efforts to address this significant threat. Our work to investigate and prosecute the unauthorized disclosure of classified material is grounded in an expansive statutory framework. The cornerstone of this framework is 18 U.S.C. § 793, which covers many leaks of classified information. Section 793 prohibits the disclosure of information "relating to the national defense" to a person not entitled to receive it. The Supreme Court, in *Gorin v. United States,* interpreted "relating to the national defense" to cover all matters directly and reasonably connected with the defense of the United States against its enemies. 312 U.S. 19, 28 (1941). The Court defined "national defense" as "'a generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness.'" *Id.* Later cases have held that this definition of "national defense" is not limited to military matters. *See, e.g., United States v. Truong Dinh Hung*, 629 F.2d 908, 918 (4th Cir. 1980) (citing *United States v. Boyce*, 594 F.2d 1246 (9th Cir. 1979)).

There are several other statutes that proscribe the unauthorized disclosure of classified information in various ways. For example, the "Intelligence Identities Protection Act," 50 U.S.C. § 421, prohibits the disclosure of the names of covert intelligence agents. Also prohibited by statute is the unauthorized disclosure of information relating to communications intelligence activities and cryptographic systems, 18 U.S.C. § 798; the unauthorized disclosure of diplomatic codes or matter prepared in any such code, 18 U.S.C. § 952; the unauthorized disclosure of, receipt of, and tampering with restricted data pertaining to nuclear material and atomic weapons, 42 U.S.C. §§ 2274 to 2277; and the unauthorized disclosure of personal information residing in an agency's records system, 5 U.S.C. § 552a. These statutes provide broad coverage for the prosecution of cases involving leaks of sensitive information.

The Department of Justice takes a lead role in the investigation and prosecution of leak cases. Executive Order 12958, as amended, describes sanctions that may be imposed on individuals who knowingly, willfully, and negligently disclose classified information. The Standard Form 312 "Classified Information Nondisclosure Agreement," signed by all Federal employees and contractors holding security clearances, specifies that United States criminal laws and penalties for unauthorized disclosure and violations of the United States Code apply to each Federal employee and contractor who signs the agreement. Executive Order 12333, as amended, requires agencies within the Intelligence Community to report possible violations of Federal law by their employees to the Department, which includes violations of statutes relating to the unauthorized disclosure of classified information. These reports identify the classified information that was leaked, the level of classification of the leaked information (*i.e.*, secret, top secret, or SCI), and the particular article or broadcast in which the information was disseminated.

Accordingly, in the normal course, an Intelligence Community agency sends a crime report to the Justice Department's National Security Division to refer the matter for possible investigation.

The Justice Department then must assess whether an investigation should be opened as a result of the reported leak. While these determinations are necessarily fact-intensive and unique to each reported incident, the Department does follow general guidelines in making this assessment. For example, the Department usually has the referring agency, in the first instance, specify in its crime report whether it would like the Department to investigate the leak. The Department has the authority to investigate a leak regardless of whether the reporting agency desires such an investigation, but eliciting the reporting agency's determination of which leaks are sufficiently damaging to warrant an investigation helps us assess how best to use our limited investigative resources.

As part of this assessment process, the Department has, for the last 40 years, generally also required the reporting agency to answer a series of specific questions to help the Department evaluate whether an investigation would be productive. Should an investigation be deemed necessary, these questions are useful in guiding the course of that investigation.

In addition to these standard appraisal processes, the Department will open, and often has opened, investigations whenever we become aware of a leak that we believe is significant, even without a referral. Similarly, the Department occasionally opens an investigation based solely on an oral request from a senior Intelligence Community official.

Once the Department concludes that a leak investigation is warranted, that investigation is conducted by the Federal Bureau of Investigation ("FBI") in consultation with the Department's National Security Division. The National Security Division oversees and

coordinates all leak investigations. The National Security Division works closely with FBI personnel and, together with the FBI, regularly briefs the reporting agencies on the status of the investigations. In addition, the National Security Division and the FBI meet with representatives of the Office of the Director of National Intelligence periodically to discuss the status of matters referred by components of the Intelligence Community.

Despite the experience and cooperative approach of the investigating parties, leak investigations may not progress to the prosecutorial phase for a number of reasons. For example, it is common to find that leaked information has been disseminated widely throughout the Federal government. Such widespread dissemination can make investigating and identifying the source of a leak impracticable.

Further complicating investigations of unauthorized disclosures of classified information to the media is the fact that there usually are only two people who know how a leak occurred and the identity of the leaker: the leaker and the reporter to whom the information was leaked. We have interpreted the Justice Department's formal policy on obtaining information from members of the news media, codified at 28 C.F.R. § 50.10, as requiring that leak investigations focus on potential leakers rather than reporters. While this policy appropriately balances the importance of First Amendment freedoms with the strong national security interest in keeping classified information from being disclosed, it necessarily limits the prosecutor's access to the reporter who received the sensitive information. In the rare case in which the Department issues a subpoena to a reporter for information about the source of a leak, the information is not necessarily immediately forthcoming. There are often lengthy legal challenges to the subpoena, which on a rare occasion can entail a reporter electing to serve jail time for contempt rather than

comply with the subpoena. In light of these limitations and the practical realities of leak investigations, the leaker often cannot be identified beyond a reasonable doubt, as required for a successful prosecution.

When a prosecution cannot be undertaken or is not successful, administrative action by the Intelligence Community agency is an appropriate course of action to ensure that the leaker is prevented from again breaching the Government's trust through any additional leaks. The Department is not involved in conducting administrative actions in other agencies, but, within the legal limits to which we are subject, the Department does encourage and support administrative actions by Intelligence Community agencies to deter and punish those who endanger our national security by leaking classified information. For example, the FBI is authorized to share with the referring agency the results of its investigation (with limited exceptions, such as access to certain grand jury information).

In conclusion, I would like to stress again that I firmly believe that leaks of classified information harm our national security interests. Leaks endanger the lives of Americans serving overseas. They also endanger all those Americans who depend on a properly functioning intelligence apparatus to protect the homeland. Despite these substantial security consequences, there remain those who take it upon themselves to leak protected Government information. I will continue to support strongly the Department's efforts to find and prosecute those responsible for dangerous leaks, while remaining true to the First Amendment principles that are vital to our nation. I also fully support Admiral Blair's sentiments on this issue and look forward to working with ODNI and all of the agencies in the Intelligence Community to pursue these important matters by all lawful means.

Thank you for inviting me here today to address this issue. I would be happy to answer any questions.