Department of Justice

STATEMENT OF

LISA O. MONACO
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

AT A HEARING CONCERNING
UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION

PRESENTED

FEBRUARY 9, 2012

STATEMENT
OF
LISA O. MONACO
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE

BEFORE THE
SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

AT A HEARING CONCERNING
UNAUTHORIZED DISCLOSURE OF CLASSIFIED INFORMATION

PRESENTED ON
FEBRUARY 9, 2012

Madam Chairman, Mr. Vice Chairman, and Members of the Committee, thank you for the opportunity to discuss the issue of unauthorized disclosures of classified information, and to explain the efforts that the Department of Justice is making to address such disclosures. We thank the Committee for its focused attention on these issues and believe that this hearing, and past hearings on this issue, have been instructive and beneficial.

The Department of Justice well appreciates the significant damage to national security caused by unauthorized disclosure of classified information. Leaks are a serious threat to our national security and have exposed extremely sensitive Government information. Virtually all elements of the Intelligence Community have suffered severe losses due to leaks, and the Department of Justice has seen national security investigations hampered by unauthorized disclosures. Through access to classified information, adversaries may strengthen their capacity to undermine our military, compromise our assets at home and abroad, and thwart our diplomatic efforts. While there are no easy answers when seeking to prevent leaks or to catch individuals who leak classified information, we appreciate the congressional interest and repeated

interagency group support to the Department's and Intelligence Communities' efforts to address the persistent problem.

The statutory landscape providing the framework for the investigation and prosecution of leak suspects is critical to the Department's efforts. Title 18 U.S.C. § 793 provides the broadest liability for leakers of classified information. Section 793 prohibits the disclosure of information "relating to the national defense" when the person disclosing the information has reason to believe it could be used to injure the United States or to aid a foreign nation. That statutory language is not limited strictly to military matters, but applies, broadly speaking, to activities of national preparedness. In addition to § 793, several other statutes restrict the unauthorized disclosure of classified information:

- The "Intelligence Identities Protection Act," 50 U.S.C. § 421, prohibits the disclosure of the names of covert intelligence agents.
- Section 798 of title 18 prohibits the unauthorized disclosure of information relating to communications intelligence activities and cryptographic systems.
- Section 794 of title 18 prohibits the disclosure of national defense information or materials to any agent of a foreign government or to a foreign government itself.
- Section 952 of title 18 prohibits the unauthorized disclosure of diplomatic codes or any information prepared in such codes.
- Sections 2274 through 2277 of title 42 prohibit the unauthorized disclosure or receipt of certain information related to nuclear materials and weapons.
- Section 552a of title 5 establishes criminal penalties for the unauthorized disclosure of personal information retrieved from an agency's system of records.

Another tool available in the fight against the leaking of classified and other sensitive information is the Federal computer hacking statute, the Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1030). Section 1030(a)(1) criminalizes computer espionage, specifically the accessing of protected national defense or foreign policy information without authority or in excess of authorization and the subsequent disclosure of that information where the wrongdoer has reason to believe that the information either could be used to injure the United States, or could be used to the advantage of a foreign nation. Section 1030(a)(2) creates a similar prohibition, but it applies to all types of information (not just classified information), obtained for any purpose. Section 1030(a)(2) can thus be useful to the Department of Justice in instances where, for example, the information wrongfully accessed is sensitive and implicates national security, but is not classified. As you know, there have been proposals to restrict the CFAA, and we look forward to discussing the proposed changes and their potential to affect our efforts to contain and prosecute leaks of sensitive information.

There is an established process for investigating and prosecuting leak cases. Executive Order 12333 requires that the Intelligence Community report violations of Federal law, including the unauthorized disclosure of classified information, to the Department of Justice. These reports come in the form of a letter identifying the classified information that was subject to unauthorized disclosure, the level of classification of the leaked information (*e.g.*, Secret, Top Secret, Codeword), and the particular article or broadcast in which the information was disclosed. These crime reports come to the Department's National Security Division and typically represent the first step to initiating a criminal investigation.

After receipt of a crime report, the Department must determine whether it should initiate a criminal investigation, to be conducted by the Federal Bureau of Investigation ("FBI"), of the unauthorized disclosure referral. The crime reports specify whether the reporting agency requests that the Department investigate the leak. The affected agencies do not seek criminal investigations of every leak; they tend to request investigations of only the most damaging unauthorized disclosures. Although the Department has the authority to commence a leak investigation even if not requested by the reporting agency, due to the nature of the investigations, our practice has been to rely on the advice of the reporting agency regarding which cases are sufficiently damaging to warrant an investigation.

In assessing whether to open an investigation, the Department has generally required that the reporting agency provide answers to a series of specific standard questions. These answers, provided after a preliminary internal review by the agency, help the Department, and its investigators at the FBI, assess whether a criminal investigation of the unauthorized disclosure would be productive. The agency's responses also help guide an investigation should one be initiated. For example, the questions require the agency to identify specifically the leaked information, including any source documents, and to make a good faith estimate of the extent of dissemination of the information. The scope of dissemination is an important element in the evaluation of the disclosure for investigation, but there are no bright-line dissemination cut-offs used in this assessment. There are, of course, instances where a significant leak occurs and the Department opens an investigation without receiving a formal crime report or before receiving answers to the specific questions. Similarly, investigations have been opened in the past based on an oral request from a senior Intelligence Community official.

Recent changes instituted by the Office of the Director of National Intelligence ("ODNI") have streamlined the process through which crime reports are submitted by the Intelligence Community agencies. The crime reporting process now utilizes a "tiered" approach. Instituted in May 2011, agencies are required to assess all unauthorized disclosures and categorize the crime report as a "Tier 1," "Tier 2," or "Tier 3" disclosure. Tier 1 disclosures are those where a preliminary review by the reporting agency reveals that further investigation is not warranted, often due to wide dissemination of the disclosed information. In this instance, the crime report does not ask for further action from the Department. Tier 2 disclosures are those where, after an internal review, the reporting agency determines that an internal, or administrative investigation, rather than a criminal investigation, is appropriate. Tier 3 disclosures are those in which the agency requests a criminal investigation. In practice, this new approach has resulted in reporting agencies taking a more structured approach to the reporting of disclosures during the preliminary review stage and thus providing a better assessment of the leak for the Department. In addition, because notice is provided in all three "tiers," there is ample opportunity for the Department to explore any interest in a criminal investigation of a Tier 1 or Tier 2 report.

After the Department determines that a criminal investigation is appropriate, the FBI conducts the investigation in consultation with the Department's National Security Division ("NSD"). NSD oversees and coordinates leak investigations and works closely with FBI personnel on these cases. NSD and the FBI regularly brief the reporting agencies on the status of the investigations and have regular consultations concerning unauthorized disclosures in which requests for investigation have been made. Additionally, NSD has periodic meetings with ODNI

representatives to discuss the status of unauthorized disclosures referred by components of the Intelligence Community.

One inherent difficulty in leak cases is that the investigations are focused on the pool of individuals who had access to the information, and not those to whom the information was disclosed. This is reflective of the fact that while there are certainly significant national security and law enforcement equities at play in unauthorized disclosure cases, there is also a need to recognize the serious First Amendment interests implicated whenever the media becomes involved in a criminal investigation. To that end, a longstanding Department regulation, codified at 28 C.F.R. § 50.10, governs contacts with media entities as witnesses, subjects, or targets, and generally limits the investigators' access to the reporters who receive classified information. While this practice undoubtedly makes these investigations more challenging, it represents a longstanding policy judgment that balances First Amendment freedoms with the strong national security interest in investigating unauthorized disclosures.

With regard to the conduct of the investigations, it bears noting that recent advances in technology have provided new opportunities for investigators, in terms of both identifying leak suspects and building successful prosecutions. In particular, some Intelligence Community agencies have enhanced their ability to audit information technology systems, allowing investigators in some instances to obtain important information regarding the timing and scope of access to classified information by potential subjects. Improved tools—including auditing measures, employee physical access or badging records, and phone records—play an important role in internal investigations and aid in unmasking individuals who leak classified information. The Department applauds and encourages the continuing progress in this area. However, even

given cooperation between agencies and the Department, as well as the increased use of technology and internal investigative techniques, pinpointing the guilty party can often be difficult following widespread dissemination of information across agencies throughout the Government and the myriad avenues leak perpetrators may utilize to communicate. Such widespread dissemination can make identifying the source of a leak essentially impossible.

When a leak investigation does progress to the prosecution phase, that prosecution invariably will call for application of the Classified Information Procedures Act ("CIPA") to regulate the discovery and use of classified information in the case. Enacted in 1980, CIPA establishes pretrial, trial, and appellate procedures for Federal criminal cases in which there is a possibility that classified information may be disclosed. CIPA allows the Government to obtain from the court a determination regarding what classified information will be subject to disclosure before any such disclosure is made, and allows the Government to seek substitutions, summaries, or stipulations in lieu of disclosure of the classified information. The Government may also seek protective orders prohibiting the disclosure of classified information. Moreover, CIPA provides procedures through which a criminal defendant can use classified information in a framework that protects the information from unnecessary public disclosure. Section 9 of CIPA provides for Department of Justice security specialists who act as Classified Information Security Officers (CISOs). Detailed to the court in a neutral capacity, the CISOs serve as advisors to the court and defense counsel and are largely responsible for the protection of the classified information during the course of the judicial proceedings.

CIPA is an exceptionally useful tool in the prosecution of national security cases and provides a carefully crafted balance between the Government's need to know what classified

information will be disclosed at a trial and the rights of the accused to mount a full, vigorous defense. CIPA has been used extensively in the last thirty years in a variety of criminal cases, and while the nature of unauthorized disclosure cases presents particular challenges, without CIPA the Government simply could not obtain criminal convictions in certain cases involving national security matters while simultaneously protecting the classified information necessarily involved in such matters.

When a prosecution is not pursued or is unsuccessful, administrative remedies by the reporting agencies are an option that is, and should continue to be, utilized against individuals who leak classified information. The Department does not conduct these administrative inquiries but does encourage, and within the legal limits to which it is subject, support administrative actions by Intelligence Community agencies. These administrative measures can be more effective and more timely than criminal prosecution, and they pose less risk of additional disclosure of sensitive information. In this way, they are useful in both deterring and punishing those who commit unauthorized disclosures of national security information.

Unauthorized disclosures of classified information cause significant damage to our national security, and the Department is always striving to enhance our ability to combat leaks while also protecting the First Amendment principles that are vital to our nation. The Department appreciates the Committee's interest in this subject, and we will continue to work with our partners in the Intelligence Community to prevent leaks.

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