~~SECRET//NOFORN~~

Statement for the Record on the

Unauthorized Disclosures of Classified Information

Senate Select Committee on Intelligence

Robert S. Litt

General Counsel

Office of the Director of National Intelligence

9 February 2012

~~SECRET//NOFORN~~

Senate Select Committee on Intelligence

Statement for the Record

Unauthorized Disclosures of Classified Information

By

Robert S. Litt

General Counsel, Office of the Director of National Intelligence

February 9, 2012

(U) Good afternoon Chairman Feinstein, Vice Chairman Chambliss, and distinguished committee members. I am pleased to appear before you to discuss the efforts of the Director of National Intelligence, and the Intelligence Community as a whole, to address the unauthorized disclosure of classified information.

(U//~~FOUO~~) This is an area of great personal importance to me. The unauthorized disclosure of our nation's secrets to the media causes genuine damage to our national security, both in individual cases where we have been able to identify actions by our adversaries that have apparently been stimulated by leaked information, and because the steady stream of leaks creates a culture that does not appropriately honor secrecy when it is essential. This Administration has been historically active in pursuing prosecution of leakers, and the Intelligence Community fully supports this effort. As we have discussed before, however, prosecution of unauthorized disclosure cases is often beset with complications, including difficult problems of identifying the leaker, the potential for confirming or revealing even more classified information in a public trial, and graymail by the defense. And looming over this entire process is an inherent tension between

protecting secrecy and fundamental Constitutional guarantees of free speech and a fair trial. The potential harm wrought by additional disclosures in a prosecution may sometimes outweigh the good that comes from the attempt to vindicate the law, and seeking safeguards for that information pursuant to the Classified Information Procedures Act may conflict with commonly understood fair trial rights of a criminal defendant, such as the right to confront witnesses. CIPA is an essential tool for protecting our secrets in court, but no law, however carefully crafted, could eliminate these issues.

(U//~~FOUO~~) Director Clapper recognizes these challenges. As a result, in May of last year he issued direction to the Intelligence Community agencies to pursue administrative investigations and sanctions against identified leakers wherever appropriate. Pursuant to this DNI directive, individual agencies are instructed to identify those leak incidents that are ripe for an administrative disposition after consulting with the Department of Justice. By advocating for administrative action in appropriate cases, the DNI hopes that more leakers will be sanctioned, and others similarly situated will be deterred.

(U//~~FOUO~~) The DNI also recognizes the importance of oversight of leak investigations that are ongoing throughout the IC. Accordingly, his memorandum directed the reporting of *all* instances of alleged unauthorized disclosure where a preliminary administrative investigation has been opened. The DNI, acting through the Security Directorate of the Office of the National Counterintelligence Executive (ONCIX/S), also tracks all leak referrals, including those cases that have been referred to the FBI for criminal investigation. Included in this oversight is an initiative for ONCIX/S

to monitor cases declined by the Justice Department for criminal investigation or prosecution. ONCIX/S will review each instance of declination with the victim agency and mutually determine if there are any additional actions that can be taken by the agency. This oversight allows the DNI to monitor the progress of all investigations and fulfill his responsibility as the Security Executive Agent responsible for safeguarding classified information.

(U//~~FOUO~~) The emphasis on administrative dispositions of leak investigations is being coupled with an effort specifically designed to beef up our efforts to deter insiders who seek to pass classified information, and identify them when they do. To that end, the DNI now co-chairs, along with the Attorney General, an Insider Threat Task Force, which has been established by a recently promulgated executive order. The task force is developing a government-wide program for insider threat detection and prevention to improve protection and reduce potential vulnerabilities of classified information from exploitation, compromise, or other unauthorized disclosure.

(~~S//NF~~) While difficult, the ability to detect behaviors and activities associated with unauthorized disclosures is vital. In this post-WikiLeaks era, where the vulnerability of our systems and the information they carry has become apparent, it is incumbent on the IC to protect our secrets while still ensuring that the right information is delivered to the right people at the right time. We applaud the passage of Section 402 of the Intelligence Authorization Act For Fiscal Year 2011, which directs the DNI to establish an effective automated insider threat detection program for the information resources in each element of the IC. The DNI also supports the efforts of the ONCIX/S as

it works to identify "best practices" for the technical auditing and monitoring of classified computer networks. ONCIX/S is moving forward to incorporate these "best practices" across the Intelligence Community to the maximum extent possible. Strengthening relationships among the security, counterintelligence and information assurance elements within these agencies will not only help root out leakers, but will also improve our overall counterintelligence profile.

~~(S//NF)~~ One of the "best practices" is maintaining solid audit data with respect to classified information. An effective audit trail that tells us who accessed classified information and when, coupled with other relevant data [redacted] represents an important step in helping us identify those who compromise our secrets. Better evidence that identifies leakers increases the likelihood of successful administrative actions and criminal prosecutions.

(b)(1)
(b)(3)

~~(S//NF)~~ At present, each individual member of the IC has audit and monitoring capabilities for their systems and networks. While there is some variance, robust programs are in place [redacted]. These programs include the ability to monitor [redacted].

(b)(1)
(b)(3)

Other agencies have less mature programs but some ability to track employee online activity. [redacted].

(b)(1)

~~(S//NF)~~ To determine if agencies are collecting useful information, ONCIX/S conducted a case review with the [redacted] to determine if any [redacted] had been hampered by the lack of requested audit data. In reviewing cases managed by [redacted] and the [redacted] there were no instances where an agency could not provide the requested audit information.

~~(S//NF)~~ Further, automated systems are being studied, developed and tested that will assist in identifying classified information published on the internet. Once information is on the internet we have no control over it, [redacted]

(b)(1)
(b)(3)

[redacted]

~~(S//NF)~~ Beginning in March 2008, ONCIX/S initiated a review of commercial and government products that could [redacted]. Market surveys indicated that at least [redacted] sold software that, with some modification, provided the required capabilities. To ensure that the ONCIX/S approach was practical and cost effective using available technology, a task order was issued to have the [redacted]

(b)(1)
(b)(3)

(b)(3)

(b)(3)

[redacted] perform a feasibility study. The [redacted] study concluded that it would be beneficial and feasible for ONCIX/S to implement a centralized and automated capability to identify potential unauthorized disclosures of classified information published electronically in the public domain, specifically the Internet. At present time, funding is being identified to contract for a pilot of the available technology as the next step of this project.

(U) In addition to encouraging administrative actions against leakers and promoting the development of an insider threat program, any comprehensive strategy to discourage unauthorized leaks must include robust training and education. ONCIX/S has developed web-based training modules for all individuals with access to classified information, as well as the security professionals who respond to leak incidents. The module for all cleared individuals emphasizes their obligation to protect classified information, identifies the harm to national security resulting from unauthorized disclosures, and re-affirms the DNI's commitment to deter unauthorized disclosures and mitigate their harm. The module for security professionals provides comprehensive guidance on the updated policy for responding to unauthorized disclosures. We intend to disseminate these modules throughout the IC and to direct that training on this subject be an annual requirement for those who maintain access to our classified information.

(U/~~FOUO~~) Preventing the disclosure of classified information to unauthorized persons remains a persistent challenge for the IC. Thousands of government employees and contractors legitimately require access to this information, and even one such individual, acting without authorization, can cause significant damage to national

security. Further, in this era of the 24-hour news cycle, classified information is linked, often inextricably, with current events playing out in real time. The appetite for information is ever more voracious, and the temptations by some untrustworthy individuals to disclose, for personal benefit, what should not be disclosed remain undiminished. We do not harbor any belief that we can halt all disclosures of classified information. Nevertheless, through the efforts we have described—the promotion of administrative sanctions, the development of insider threat capabilities, and the education of the IC work force—we are sending a larger message to potential leakers and ensure that all information that needs protecting is safeguarded for the security of our Nation.

(U) I thank you for your time and look forward to answering any questions.