Written by **Joe Wolverton, II, J.D.** on April 12, 2012

President Creates Task Force to Stop Leaks of Classified Information

The proposal is a requirement of an executive order signed October 7 of last year by President Obama. Executive Order 13587 sets guidelines designed to "to ensure the responsible sharing and safeguarding of classified national security information (classified information) on computer networks."

One step toward the accomplishment of this goal is the creation of an interagency Insider Threat Task Force. That group is charged with developing

> a Government-wide program (insider threat program) for deterring, detecting, and mitigating insider threats, including the safeguarding of classified information from exploitation, compromise, or other unauthorized disclosure, taking into account risk levels, as well as the distinct needs, missions, and systems of individual agencies. This program shall include development of policies, objectives, and priorities for establishing and integrating security, counterintelligence, user audits and monitoring, and other safeguarding capabilities and practices within agencies.

Reading between the lines it is easy to see what prompted the issuing of this order and the creation of this new bureaucracy: WikiLeaks.

President Obama likely was also motivated by the acts of Army Private Bradley Manning. In what is described as "the biggest leak of classified information in U.S. history," Manning is accused of passing over 700,000 documents and video clips to WikiLeaks, the widely known website devoted to exposing government corruption throughout the world.

Private Manning, 24, from Crescent, Oklahoma, has been detained since he was arrested on May 29, 2010 while on deployment with the 10th Mountain Division in Iraq. While on duty near Baghdad, Manning had access to the Secret Internet Protocol Router Network (SIPRNet) and the Joint Worldwide Intelligence Communications System. SIPRNET is the network used by the U.S. government to transmit

classified information.

Manning's arrest came as the result of information provided to the FBI by a computer hacker named Adrian Lamo. Lamo told agents that during an online chat in May 2010, Manning claimed to have downloaded classified information from SIPRNet and sent it to WikiLeaks.

According to published reports, the material Manning is accused of unlawfully appropriating includes a large cache of U.S. diplomatic cables (approximately 250,000), as well as videos of an American airstrike on Baghdad conducted in July 2007 and a similar attack in May 2009 on a site near Granai, Afghanistan (an event sometimes known as the Granai Massacre).

Of course, the new policy is being promoted by the Obama administration as an attempt to assist law enforcement and intelligence to "connect the dots" so as to prevent future terrorist attacks on the homeland.

A key member of the task force and the Office of the Director of National Intelligence, John Swift, is quoted in a recent article as saying that the agencies named in the executive order are committed to conforming to the requirements handed down by President Obama.

"The National Policy on Insider Threat is in draft and will probably move its way to the White House National Security Staff in the next month or two, which is pretty fast in the federal scheme of things," said Swift during a panel discussion on the insider threat at the FOSE trade show in Washington Wednesday. "However, in order to actually implement a program, you will want to have standards. Those standards are being developed now by the task force, and all the interagency members that are working on it. Those standards have to be issued by October of this year."

The Order gives the agencies one year to set and implement the appropriate standards for identifying and eliminating the threats of leaks caused by intelligence insiders.

According to the article published by Federal News Radio, Swift said that most agencies have already developed protocols for identifying "troubled employees" who would be the most likely suspects in a case of an insider passing on classified information.

The Task Force will take advantage of the protocols that are already in place by examining each and choosing from among them those best suited to being reported to all the relevant departments within the Executive Branch.

In reading the description of the policy in the Federal News Radio piece, it would seem that the Task Force is preparing training modules for federal employees that teach them how to recognize behavior that might indicate that a colleague is a potential risk to national security.

Prior to the branch-wide implementation of whatever scheme is finally approved by the Task Force and the President, there is a method already set to be enforced that could address the potential for leaks.

In order to decrease the "potential for terrorist attacks," Homeland Security Presidential Directive 12 calls for the creation of a

> a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

Rob Carey, the Defense Department deputy chief information officer, said during another session at FOSE that the federal ID card can "prevent unauthorized access to data and promote information sharing at the same time along with improving the cybersecurity of an agency's network."

The absolute requirement that the identification be used by intelligence employees will provide the President with a keystroke-by-keystroke record of every worker's online activity. This level of after-the-fact monitoring will plug the pores in our nation's cybersecurity.

As Carey explained it, implementation of the key card control mechanism will "add another layer of security while also letting officials know who is on the network, when they were on the network and what they were doing there."

As set forth in the Directive:

> "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application.

The use of the "Common Identification Standard for Federal Employees and Contractors" is only one of the ideas being offered for securing the country's most critical classified data.

One member of the Insider Threat Task Force, Diana Braun, said that the ID cards are just one of five "near term ways to strengthen systems against insider threats."

According to the rubrics contained in Executive Order 13587, the agencies listed therein must submit annual reports to the Steering Committee created by the Order.

The Senior Information Sharing and Safeguarding Steering Committee:

> shall be co-chaired by senior representatives of the Office of Management and Budget and the National Security Staff. Members of the committee shall be officers of the United States as designated by the heads of the Departments of State, Defense, Justice, Energy, and Homeland Security, the Office of the Director of National Intelligence, the Central Intelligence Agency, and the Information Security Oversight Office within the National Archives and Records Administration (ISOO), as well as such additional agencies as the co-chairs of the Steering Committee may designate.

While it is indisputable that our nation must be protected from the damage that could be caused by intelligence agency insiders who criminally pass classified information to those who could pose a legitimate and demonstrable threat to our national security, what is perhaps more helpful to the long-term freedom of our Republic is the immediate end of all those secret yet reprehensible activities being carried out by our government that bring shame to every citizen.

If we could rid our government of those in high places who are working against the cause of liberty and peace, then we wouldn't need another task force or federal agency.