17 October 2017

WikiLeaks Task Force

Final Report

[redacted]

Intelligence Brief

Intelligence Brief

17 October 2017

[redacted] **Memo To:** **Director, Central Intelligence Agency**
Deputy Director, Central Intelligence Agency
Chief Operating Officer, Central Intelligence Agency

[redacted] **From:** **WikiLeaks Task Force,** [redacted]

[redacted] **Subject:** **WikiLeaks Task Force Final Report**

[redacted] Executive Summary

[redacted] WikiLeaks' announcement on 7 March that it possessed cyber tools from CIA's Center for Cyber Intelligence (CCI), dubbed "Vault 7," marked the largest data loss in CIA history. In its initial public disclosure, WikiLeaks provided the names and brief descriptions of multiple tools that CIA developed for cyber operations. Since 7 March, WikiLeaks has published more comprehensive descriptions of 35 tools, including internal CIA documents associated with each tool. [redacted]

- [redacted] We assess that in spring 2016 a CIA employee stole at least 180 gigabytes to as much as 34 terabytes of information. This is roughly equivalent to 11.6 million to 2.2 billion pages in Microsoft Word. This data loss includes [redacted] cyber tools that resided on the Center for Cyber Intelligence (CCI) software development network (DevLAN). We cannot determine the precise scope of the loss because, like other mission systems[a] at that time, DevLAN did not require user activity monitoring or other safeguards that exist on our enterprise system.
- [redacted]
- [redacted] To date, WikiLeaks has released user and training guides and limited source code from two parts of DevLAN: Stash, a source code repository, and Confluence, a collaboration and communication platform. All of the documents reveal, to varying degrees, CIA's tradecraft in cyber operations.

[redacted]

[redacted] This product is intended for internal Agency use. [redacted]

[a] We define a mission system as any computer-based capability that collects, stores, processes, or communicates information that is managed by a mission component [redacted]

[redacted]

[redacted] Critical Context

[redacted] **CCI:** The WikiLeaks breach occurred at CCI, whose mission is to transform intelligence through [redacted] cyber operations. It would be unfair to lay the blame for the breach with the current management, as the breach occurred before most joined CCI. Equally, CCI correctly notes that the mission system in question complied with all Agency requirements at the time of the breach. However, in a press to meet growing and critical mission needs, CCI had prioritized building cyber weapons at the expense of securing their own systems. Day-to-day security practices had become woefully lax. The Development Network (DevLAN) on which CCI's work product resided had been certified and accredited, but CCI had not worked with CIMC to develop or deploy user activity monitoring or robust server audit capability. Most of our sensitive cyber weapons were not compartmented, users shared systems administrator-level passwords, there were no effective removable media controls, and historical data was available to users indefinitely. Furthermore, CCI focused on building cyber weapons and neglected to also prepare mitigation packages if those tools were exposed. These shortcomings were emblematic of a culture that evolved over years that too often prioritized creativity and collaboration at the expense of security.

[redacted]

[redacted] **Mission Systems:** CIA has moved too slowly to put in place the safeguards that we knew were necessary given successive breaches to other US Government agencies. For nearly a decade WikiLeaks has exploited the digital realm to profoundly reshape opportunities for individuals sworn to protect our nation's secrets to leak classified or sensitive information. While CIA was an early leader in securing our enterprise information technology (IT) system, we failed to correct acute vulnerabilities to our mission IT systems. Because the stolen data resided on a mission system that lacked user activity monitoring and a robust server audit capability, we did not realize the loss had occurred until a year later, when WikiLeaks publicly announced it in March 2017. Had the data been stolen for the benefit of a state adversary and not published, we might still be unaware of the loss—as would be true for the vast majority of data on Agency mission systems.

— [redacted] The Agency for years has developed and operated IT mission systems outside the purview and governance of enterprise IT, citing the need for mission functionality and speed. While often fulfilling a valid purpose, this "shadow IT" exemplifies a broader cultural issue that separates enterprise IT from mission IT, has allowed mission system owners to determine how or if they will police themselves, and has placed the Agency at unacceptable risk.

[redacted]

[redacted]

[redacted] This wake-up call presents us with an opportunity to right longstanding imbalances and lapses, to reorient how we view risk, [redacted]. We must recognize when we are taking smart risks and when operational shortcuts or waivers create unwarranted risk to our work and to the Agency. We must care as much about securing our systems as we care about running them if we are to make the necessary revolutionary change.

[redacted]

[redacted] Recommendations

[redacted]

[redacted] The WikiLeaks Vault 7 disclosures have brought to light multiple ongoing CIA failures that our recommendations are designed to address:

- [redacted] We failed to equip the mission system in question with user activity monitoring and robust server audit capability, which could have deterred, detected, and possibly prevented the theft. [redacted]
- [redacted] We failed to empower any single officer with the ability to ensure that all Agency information systems are built secure and remain so throughout their life cycle. Because no one had that ability, no one was accountable—and the mission system in question, like many [redacted] others, lacked appropriate security. [redacted]
- [redacted] We failed to ensure that our ability to secure our information systems against emerging threats kept pace with the growth of such systems across the Agency. [redacted]
- [redacted]
- [redacted]
- [redacted] We failed to recognize or act in a coordinated fashion on warning signs that a person or persons with access to CIA classified information posed an unacceptable risk to national security. *(See recommendations B1, B2, B3, B4, B6, B7, B8, B9, and C8.)*

[redacted]

[redacted]

[b] A "zero-day" exploit is software designed to exploit a previously unknown or unpatched computer vulnerability.

Recommendation A5:

Enhance information technology security guidelines and classified information handling restrictions for zero-day exploits and offensive cyber tools, consistent with Executive Order 13526, Classified National Security Information. We judge the vulnerability of and threat to this information is exceptional and warrants additional security protections, to include requiring segmentation of knowledge, tools, and people through physical and logical infrastructure, policy and procedural controls, and enforcing strict need-to-know access to the tools and exploits.

[redacted]

[redacted] The WikiLeaks disclosures revealed resource-driven gaps and weaknesses in CIA's insider threat program. There have been seams in communication between components such as the Office of Medical Services, Human Resources, Security, Counterintelligence Mission Center, and line management that have sometimes prevented us from connecting the dots to corporately detect and address insider threats. [redacted]

— [redacted] We have been slow—due to resource choices and cultural resistance—to extend state-of-the-art audit and user activity monitoring technology to mission systems not connected to the main enterprise network. [redacted]

[redacted] Recommendation [redacted]

[redacted] Frequent personnel security reviews and training have focused on enterprise "privileged users," defined as individuals designated and entrusted by managers to perform elevated functions on a network, system, or application. This does not include privileged users on mission systems or those with extraordinary access or capabilities, such as EDG developers. [redacted]

[redacted]

[redacted]

Data in Confluence, a collaboration and communication platform, and some data in Stash, a source code repository, have been released by WikiLeaks; we assess WikiLeaks possesses all of the Confluence and Stash data.[51] However, we now assess with moderate confidence that WikiLeaks does not possess the Gold folder of final versions of all developed tools and source code that resided on the Development Network (DevLAN), even though WikiLeaks claims it has released only a small slice of the archive it possesses. The Gold folder was better protected; WikiLeaks so far has released data in Stash despite the availability of newer, easier to exploit versions of tools in Gold; and Gold's size, several terabytes, made it harder to export.

[redacted]

[redacted] We are making educated assumptions about the scope and timing of the loss, in part because we lacked effective monitoring and auditing of this mission system. [redacted]

[redacted]

The WikiLeaks disclosures revealed gaps and weaknesses in CIA's Insider Threat program, which has traditionally relied on close coordination between the Office of Security and CIMC. Among the gaps are the seams in communication between components such as the Office of General Counsel, Medical Services, Human Resources, security, counterintelligence, and line management that have sometimes prevented us from connecting the dots to corporately detect and address Insider Threat issues. [redacted]