Cyberspace and Agility: Lessons from the Office of Personnel Management Breaches

David Alberts

The Challenge: When Office of Personnel and Management (OPM) data breaches affected 21 million Federal employees with security clearances, the Federal government turned to the Department of Defense to lead the near-term response and develop a long-term solution. The long-term solution requires a top-to-bottom transformation of the security clearance vetting ecosystem.

The Breaches and Their Significance

In June 2015, many current and former members of the Department of Defense workforce learned from two news reports that the Office of Personnel Management (OPM) had suffered at least two data breaches that could adversely affect them and their families. Federal officials characterized these breaches as among the largest breaches of government data in the history of the United States. As it turned out, the data compromised contained not only personally identifiable information (PII) such as Social Security numbers, but also fingerprint and security clearance-related information that employees, contractors, and applicants had provided on the Standard Form 86, Questionnaire for National Security Positions.

For the workforce, the breaches, subsequent announcements by Federal officials, Congressional testimony, and news stories regarding the breaches certainly did not instill a sense of confidence in the security of their information nor in the adequacy of the Federal response. Perhaps most alarming was that initial announcements of the number of people adversely affected grew from 4.2 million to more than 21 million.

Not only were DoD employees and contractors the victims of these attacks, but the compromise of sensitive information collected during security background investigations has serious national security implications.

Upon learning the extent of these attacks, senior leaders across the government dedicated themselves to better understanding the nature of these cyberattacks, taking steps necessary to prevent future intrusions, notifying the individuals affected, and offering them both identity protection and credit monitoring services. With more than 80 percent of the individuals who undergo security-related vetting, DoD was the agency most affected by the OPM breaches. Not only were their employees and contractors the victims of these attacks, but the compromise of sensitive information collected during security background investigations has serious national security implications. One can easily imagine how this information could be used by a sophisticated nation-state actor.

The DoD Response

With the charge to respond rapidly, DoD was given the responsibility to lead an interagency effort to notify affected individuals and arrange for appropriate services. In July 2015, the DoD Chief Information Officer (CIO) formed a Notifications Tiger Team, led by the Deputy CIO for Cybersecurity, to plan and manage this effort. The objective was to notify those affected as promptly as possible, while protecting against any additional compromise of this information and the possibility of adversary counterintelligence exploitation.

IDA supported the DoD Notifications Tiger Team in several ways. These included identifying what tasks were needed and assessing, in real time, progress in identifying critical path items that needed immediate attention. IDA also provided support to the efforts to bring on board a contractor to provide credit monitoring and identity theft protections by developing a statement of work, formulating evaluation criteria, and serving as advisors to source selection and later security reviews to help ensure that personal and sensitive data would be appropriately protected.

The DoD-led interagency effort to notify those affected by the second OPM breach resulted in letters being sent to more than 90 percent of these individuals by mid-December 2015, less than six months after the Tiger Team was formed and less than three months from award of the credit monitoring and identity theft contract. The team met its principal objectives of notifying affected individuals while safeguarding sensitive information, despite an extremely aggressive schedule and the need to overcome a number of potentially mission-threatening challenges.

Need for Transformation

Based on what was learned from the post-breach efforts, it became clear that a top-to-bottom transformation of security clearance vetting ecosystem would offer the best chance to reduce the frequency and severity of future intrusions and compromises, as well as address significant shortcomings of the existing process and systems. IDA developed the following vision statement for a transformed vetting ecosystem:

> *A transformed end-to-end process supporting security, suitability and credentialing (SSC), Insider Threat, and CI that leverages the power of information technology, ubiquitous data, and automation operating in a secure, defended, agile, shared infrastructure.*

This vision was subsequently adopted by the interagency group that oversees and coordinates the Federal vetting enterprise.

As shown in Table 1, IDA compared and contrasted the capabilities and characteristics of current concepts based on legacy technologies to a transformed concept enabled by newer technologies.

This description of a transformed ecosystem vision involves more than a better information technology system and more than a re-engineered process. It is, first and foremost, an *agile* ecosystem that addresses the vetting challenge in a holistic manner, with the capability to learn from streams of real-time information, learn what works and what does not, and evolve its governance and design to seize upon opportunities for improvement and respond to stresses as circumstances change.

IDA continues to support the Under Secretary of Defense for Intelligence and the DoD CIO as DoD develops the new National Background Investigation Service. Also, OMB asked IDA to perform an agility-based analysis of the security clearance vetting ecosystem to ensure that agility is built into transformational efforts.

Table 1. Current Concepts vs. Transformed Concepts

Characteristics and Capabilities	Current Concepts and Legacy Technology	Transformed Concepts Enabled by Technology
Cybersecurity	patchwork	designed and built-in end-to-end defenses evolving with threats
Workflow	fixed periodic	dynamically reconfigurable anomaly triggers
Routine Tasks Information Gathering	many prescribed, manpower-intensive	fewer, tailored automated to the extent practical
Missions	one	multiple
Protection Levels	one	as many as needed
Ability to Change / Evolve	limited high cost – not timely	agile with evidence-based evolution

Dr. David Alberts is a Senior Fellow in IDA's Strategy, Forces and Resources Division. He holds a Doctor of Philosophy in operations research from the University of Pennsylvania.