The Human Role in Institutional Cybersecurity

Vincent Pisani

Abstract

Humans have consistently proven to be a single recurring point weakness in information security and institutions must evolve to meet this reality of cybersecurity. The United States Postal Service (USPS) and United States Department of Defense (US DOD) have emerged at different ends of a spectrum, with the development of an educated government workforce and the establishment of a robust cybersecurity enterprise placed at its ends. However, modern institutions likely will have to learn from both strategies if they are to maintain the trust of stakeholders into the digital age.

*Keywords*: Cybersecurity, Humans, USG, US DOD, USPS

[Figure 1: US Government Agencies and Departments 6](#_Toc82723692)

[Figure 2: USPS Human Centric Cybersecurity Programs 6](#_Toc82723693)

Humans have consistently proven to be a single recurring point weakness in information security. This is despite the highly technical nature of this field and the large sums of money spent to fortify critical information infrastructure against intrusions. Furthermore, the institutional trust that many of us have become accustomed over the last century is not built to work in the digital age and is now beginning to negatively affect how these institutions interact with their stakeholders across the world (Wired Secuirty, 2018). The US government in particular has evolved into a complex web of interdependent agencies and departments with their own information enterprises and cybersecurity requirements (Figure 1). This has led to the emergence of several different strategies to address cybersecurity issues, with the United States Postal Service (USPS) and United States Department of Defense (US DOD) employing vastly different solutions to human centric cybersecurity challenges built around their respective missions.

The USPS has been addressing the human factor in cybersecurity through proactive cultivation of an informed workforce (Fissea, 2017). This strategy originally was implemented in response to a data breach in November 2014, which the agency’s Chief Information Security Officer (CISO) concluded was the result of a failure to foster a culture of cybersecurity across the entire agency and their failure to complying with specific legal and industry requirements in this field ((Fissea, 2017) (Wired Secuirty, 2018)USPS Office of the Inspector General, 2015). This led the USPS to further develop its cybersecurity workforce, implement training and awareness campaigns, organize stakeholder and leadership engagement campaigns, and establishing cybersecurity program governance (Figure 2). Their training campaign was further elaborated on as involving awareness-level education, role-based training, anti-phishing education, and tailored training aids. This strategy is designed to preemptively target human centric cybersecurity vulnerabilities among their workforce and address them before they become a threat.

The US DOD, on the other hand, has been building their cybersecurity infrastructure around the High-Reliability Organization (HRO) model used by the aviation and nuclear energy industries (James A. Winnefeld Jr., 2015). This model has been adopted because of the deep awareness of vulnerabilities, standards, and accountability necessary for the department’s cybersecurity enterprise to function in the face of today’s national security threats. HROs embody the principles of integrity, depth of knowledge, procedural compliance, forceful backup, questioning attitude, and formal communication to accomplish their mission and ensure continuity of operations during a time of crisis. The department’s cybersecurity planners also observed that past cybersecurity breaches have been caused by one of these principles being violated by the department’s cybersecurity personnel. As such, this strategy is primarily designed to address the trust and reliability of the department’s cybersecurity staff rather than preempting enterprise-wide human centric vulnerabilities.

The USPS and US DOD ultimately are investing in ways to address the human factor in their cybersecurity infrastructure and limit its impact on their day-to-day operations. However, they are approaching this issue in vastly different ways which have been informed by their respective missions. The USPS is an independent government agency whose primary mission is the delivery of mail and parcels. This means they are a public facing US government entity that interacts with their stakeholders every day, among which includes members public and corporations. Maintaining a high level of trust among their stakeholders is essential to the USPS’ mission because they have access to one of the largest repositories of personal information in the US Government. The USPS is primarily building trust between their employees and stakeholders through educational programs aimed at defeating social engineering-based intrusions. However; they have simultaneously developed their own cybersecurity workforce to ensure personal information is protected when a social engineering based intrusion inevitably occurs. The US DOD, on the other hand, is a much more insular government agency due to its role in the national security apparatus. This has resulted in the department placing a disproportionate level of trust in the abilities of their cybersecurity professionals rather than focusing on educational programs designed to educate their workforce. This also means that the department has primarily geared its cybersecurity apparatus toward responding to threats rather than preempting them. However, it is important to remember that the US DOD is one of the largest bureaucratic organizations in the world with different jurisdictions and requirements for personnel training across the entire organization. As such, the US DOD is unlikely to implement department wide standards and practices regarding the human factor in cybersecurity until the trust of key stakeholders has been harmed due to a high-profile intrusion.

In conclusion, the USPS and US DOD have successfully implemented mission specific institutional strategies to address the human factor in cybersecurity. However, these strategies have materialized at different ends of a spectrum that places the USPS’ educated government workforce and US DOD’s highly trained cybersecurity workforce at its extremes. Ultimately, modern institutions will have to simultaneously educate their workforce about cybersecurity threats and work to build a resilient cybersecurity enterprise to maintain the trust of their stakeholders as we progress into the digital age.

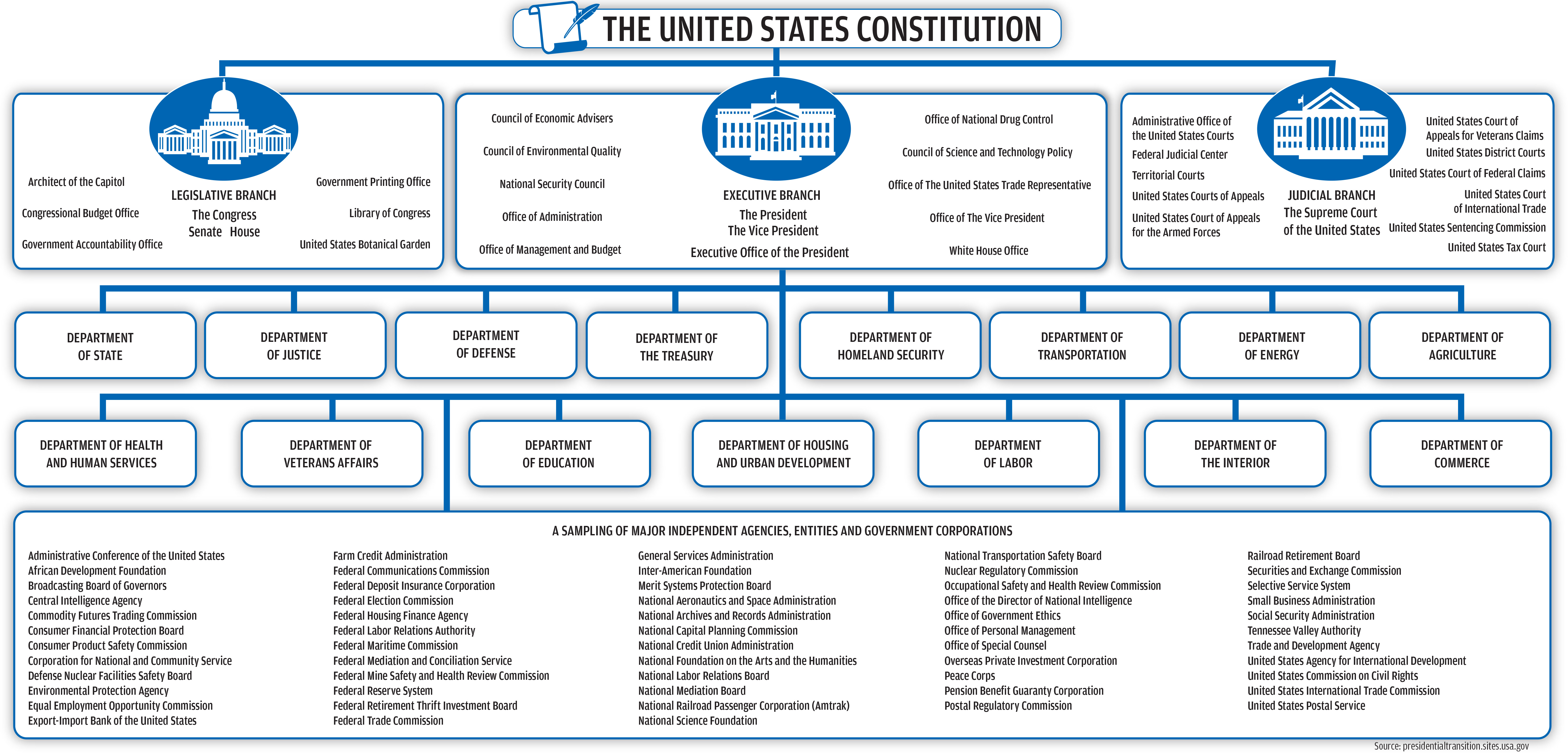


Figure 1: US Government Agencies and Departments

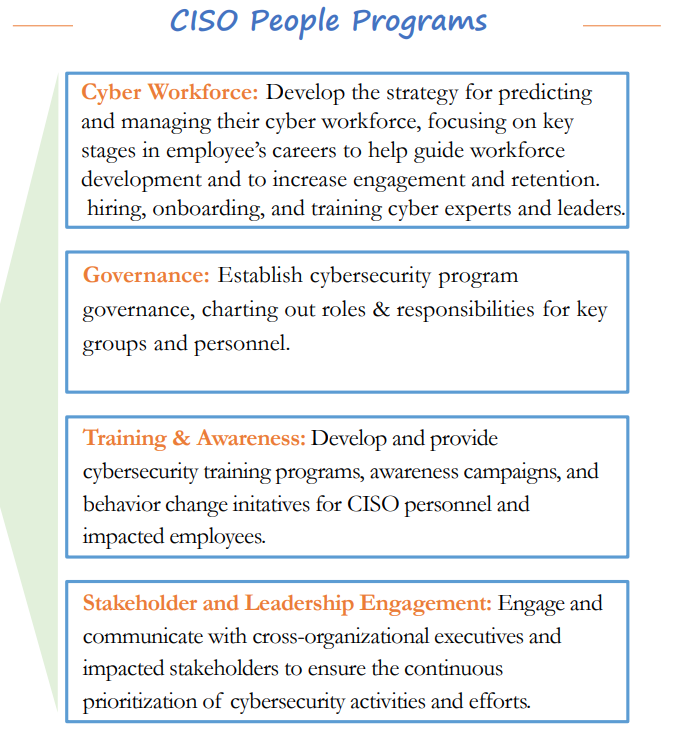


Figure 2: USPS Human Centric Cybersecurity Programs

# Bibliography

Fissea. (2017). *Cybersecurity-The Human Factor*. Retrieved from National institute of Standards and Technology: https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017\_Witkowski\_Benczik\_Jarrin\_Walker\_Materials\_Final.pdf

James A. Winnefeld Jr., C. K. (2015, September). *Cybersecurity’s Human Factor: Lessons from the Pentagon*. Retrieved from Harvard Business Review: https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon

USPS Office of the Inspector General. (2015, July 17). *Information Technology-Audit Report-15-008*. Retrieved from USPS Office of the Inspector General: https://www.uspsoig.gov/sites/default/files/document-library-files/2015/usps\_cybersecurity\_functions.pdf

Wired Secuirty. (2018, April 4th). *The Biggest Issue in Cybersecurity is Humans, Not Machines*. Retrieved from Youtube: https://www.youtube.com/watch?v=15lS2SfW4pM