Ranking Member John Katko

SOLARWINDS CAMPAIGN RESPONSE FIVE PILLAR PLAN

1 We need to seriously rethink our fragmented approach to .gov security by centralizing authority with the Cybersecurity and Infrastructure Security Agency (CISA) where possible.

While CISA's federal hunt authority from the FY2021 NDAA is a welcomed step in the right direction, CISA still does not have the proper authorities, resources, or holistic visibility into the .gov enterprise to effectively defend, and nimbly respond to, attacks.

- CISA needs resources. We cannot expect them to compete against nation-state actors with a mere fraction of the resources. As a starting place, these long overdue federal hunt authorities still need to be fully operationalized.
- We need to rethink our desired .gov security outcomes and align FISMA with those outcomes. Specifically, we need to ensure that CISA has adequate real-time visibility across the entire .gov enterprise. The EINSTEIN and CDM programs are a generally helpful baseline, but there are still significant blind spots such as cloud services.
- CISA needs investment in the underpinnings of its technological architecture to maximize the ability to distill insight across .gov.
- Ultimately, we need to empower CISA to become the operational Chief Information Security Officer (CISO) of the Federal Government. The current confederated authority model across 100+ agencies is too clunky.
- This shift should build off CISA's designation as the cybersecurity Quality Services Management Office (QSMO) of the Federal Government. Zero trust solutions should be part of this evolution.

2 We need to better understand the nature and extent of third-party cyber risks.

Very few people had even heard of SolarWinds in early December 2020, yet its products are leveraged by close to 80% of the Fortune 500 with a relationship between vendor and customer that inherently enables a high degree of administrative privilege on the host network. In this interconnected web of hardware, software, and services that underpin our way of life, where are there concentrated sources of risk that could result in cascading or systemic impact if we assume breach?

- We must better understand the ubiquity of managed service offerings with pervasive access privileges. Highly prevalent + high degree of privilege = a potentially concentrated source of risk to better understand and identify.
- The Biden Administration should leverage CISA's requirement to carry out the Continuity of Economy provision of the FY21 NDAA to illuminate where there are deployments of hardware, software, and services that present the potential for systemic risk.
- CISA should build on its existing Information and Communications Technology (ICT) element taxonomy developed in partnership with industry to specifically tease out more risk fidelity for 'sensitive system software.'

3 Once we identify the potentially concentrated sources of cyber risk, we need to ensure that vendor certification processes actually reduce that risk – not create perfunctory compliance exercises.

There are a number of vendor certification or risk judgment regimes in various stages of operationalization across the federal government, with DoD's CMMC and the Federal Acquisition Security Council (FASC) garnering the most headlines. Let's work together to ensure these regimes accomplish our common goal of actually reducing risk.

- Before we jump to create the "certification of all certifications," let's first examine the viability of pushing the existing regimes in the most productive directions.

4 We need to drive better software assurance and development lifecycle practices across the entire ecosystem.

Whether software flaws are deliberate or not, the software supply chain represents an attack vector that if exploited, leaves the potential for a "digital pandemic" of sorts – where the impact of one bad line of code can be felt across the entire economy.

- We should build on our understanding of concentrated sources of cyber risk to identify ways to verify the security of software updates that could have particularly grave consequences if compromised.
- Great work has already been done by a number of organizations to develop best practices for secure software development – such as NIST, BSA, and SAFECode – and these should be promoted and adopted more broadly.

5 We must impose real costs on cyber adversaries like China, Russia, Iran, and North Korea.

While there is no silver bullet, deterrence still matters. Naming and shaming, indictments, sanctions, offensive measures where appropriate – these should all be tools in our toolkit. From the sophisticated (nation state) to the more routine (ransomware), the cost/benefit analysis of cyber aggression still favors adversaries too often.

- Better international norms can be helpful, but they will never alone solve the problem.
- Our adversaries must understand the consequences that will come from their cyber aggression.