House Space, Science & Technology Hearing
CYBERSECURITY AT NASA: ONGOING CHALLENGES AND EMERGING ISSUES FOR INCREASED TELEWORK DURING COVID-19

OPENING STATEMENTS
Chairwoman Kendra Horn (D-OK) of the Subcommittee on Space and Aeronautics
Chairwoman Eddie Bernice Johnson (D-TX)

WITNESSES

- Mr. Jeff Seaton, Chief Information Officer (Acting), National Aeronautics and Space Administration [Truth in Testimony]
  The Honorable Paul K. Martin, Inspector General, National Aeronautics and Space Administration [Truth in Testimony]
  Diana L. Burley, PhD, Vice Provost for Research, American University [Truth in Testimony]

Chairwoman Kendra Horn (D-OK)

- NASA is a high-value target for hackers and criminals. NASA is the most attacked agency in the federal government – Jim Bridenstine said.
- Malicious actors interested in breaching NASA contractors. Protecting NASA IT and data requires vigilance.
- Multiple NASA-OIG and GAO reports identified weaknesses in NASA information security. Top agency challenge given IT supply chain risks. We need to ensure NASA has tools to have security during COVID and beyond.

Ranking Member Babin (R-TX)

- Examples of Landsat-7 experiencing cyber activities against their command-and-control system.
- NASA is not adequately securing its networks from unauthorized access from IT devices.

Mr. Seaton

- NASA employees have used virtual collaboration tools such as WebEx and Microsoft Teams. Employees are dependent on private networks to connect securely to internal networks and systems.
- Today, VPN is supporting 40,000 users with availability exceeding 99%.
- We continue to strengthen our capabilities to defend our data. Confident that NASA is strengthening response to these threats.
- Today, NASA operations span multiple centers to allow 24/7 operations even if there is a disruption. NASA is transitioning into a pro-active cybersecurity posture.

Mr. Martin

- NASA OIG issued 16 audit reports with 72 recommendations over the past 5 years. We conducted more than 120 investigation on attacks.

- Spends more than 2.4 billion a year on portfolio of IT assets including IT systems to control spacecrafts, collect scientific data.
- NASA has struggled to implement effective IT governance structure over the past two decades. Agency's CIO has limited oversight and influence over IT purchases and decisions. This decentralized nature have hindered CIO's ability. NASA connectivity with educational institutions and 3000 web domains offer cyber criminals a larger target than most government agencies.
- NASA remained at level 2/5, has not implemented policy and procedures for its IT security programs. NASA struggles to find the right balance between user flexibility and system security.
- For years, NASA permitted personal IT devices to access non-public data. NASA faces elevated risk of breach.

Dr. Burley

- Never before has seen range and volume of remote workers and remote working environments.
- We need to recognize technical needs and environmental factors (non-experienced users are at higher risk as the agency did not train users to adapt to a new remote environment)
- Needs to address the complex realities of employees' needs. Need a wholistic approach.

Q&A:

1. Chairwoman Horn (D-OK) asked on requirement to sign off on cybersecurity requirements and contracts.
2. Chairwoman Horn (D-OK) over phishing protections – Witness answered The most vulnerable part of IT is the people, so is trying to automate more.
3. Mr. Martin – NASA heading in the right direction, in the past few years: real attempt to expand. NASA is cautiously optimistic.
4. Rep. Babin (R-TX) to Seaton: President Trump signed SPD-5 which focus on Cybersecurity threshold for space systems. Seaton: Currently reviewing SPD-5, good news is a lot of consistencies with practices we're already implementing.
5. Rep. Babin –on OIG conducting audits. Mr. Martin: OIG conducts program audits and ensure IT requirements in the contracts are followed. Babin: is this a more appropriate role for the procurement office than the OIG? Martin: OIG has limited capacity like most organizations and so will try to target high value assets NASA has for a deep dive audit.
6. Rep. Babin: Video conferencing vulnerabilities? Seaton: we have a set of approved tools.
7. Rep. Perlmutter (D-CO): most vulnerable spot for hacking is the individual. When you are testifying, you talked about novice users not familiar with protocols. Personnel department is key here. What do you see being done to help the individuals help through anxious period? Dr. Burley: needs to be collab between HR and IT department. Every agency has cyber awareness programs. Those awareness programs need to be adapted to know that employees are working around other people (family, children). Human resources need to provide support to employees to focus on doing work.
8. Rep Posey (R-FL) what steps are necessary to secure supply chains from China's hackers. Martin: China is one of the foreign entities out there that is seeking NASA's intellectual property. We have conducted a series of criminal investigations when we get leads and we work with the FBI.
9. Rep Posey: Should the National academies do another study to identify opportunities? Dr. Burley: the opportunity gives us an in-depth look, I say yes.

10. Rep. Beyer (D-VA): On boarding new interns, employees. I was surprised that personally owned devices can connect to internal systems. How do you make sure new employees are given proper equipment or ensure personal devices are secure? Mr. Seaton: we do provide employees with tools they need. My office changed policy to no longer allow personal device.
11. Rep. Beyer (D-VA): what are they after (other than personally identified info)? How does this affect our missions? Mr. Martin: NASA has capital, information. Country actors are after innovation, PII, contractual data on the system. NASA is also under attacked from domestic actors.
12. Rep. Beyer (D-VA): NASA is so decentralized. Are there other examples of federal systems that are decentralized but successfully avoided this issue for NASA to emulate. Dr. Burley: there are a few but CIO would be better equipped to answer this. Mr. Seaton: There are other CIOs, we're moving in the enterprise direction significantly.
13. Rep. Garcia (R-CA): Are we able to provide government IP to the lower-level supplies so they can implement security measures in their supply chain? Mr. Seaton: Challenge to make sure all our suppliers comply with supply chain restrictions and building that into the best practices. Rep. Garcia – important to make sure suppliers are not driven out of business.
14. Rep. Weber (R-TX) intrusions this month during COVID? Mr. Seaton: we have seen an increase in phishing attacks fluctuating throughout the pandemic. One point, doubling attacks. Other weeks- lower. Because of the pandemic, people are looking the opportunity to attack.
15. Weber (R-TX) – DOD and ULA identified and cut ties with suppliers due to Chinese ownership. Shouldn't NASA take a proactive posture to know what safeguards are in place for the supply chain. Should there be some threshold and somebody to look over their shoulder? Mr. Seaton: yes. We're involved in ensuring level of compliance. How business practices – NASA doesn't get in the middle of. I think it's a shared responsibility between federal agency and an agency interacting with a specific provider. Weber wants more information on who/ which agency should be responsible to investigate this.
16. Chairwoman Horn: Personal device follow-up questions. Mr. Martin: previously NASA had a BYOD policy (bring your own device) very forward leaning. Now, have implemented software but has not adequately blocked devices to be on system or enforcing mobile devices don't violate supply chain rules.
17. Chairwoman Horn: What is NASA doing to address these holes? Mr. Seaton: we've been a leader in implementing DHS programs to detect what's on the network and we're at phase 2: controlling who's on the network.
18. Chairwoman Horn: on contractor requirements and suppliers, balancing between overburdensome requirements: what do you see as potential authorities that NASA may need to have additional insights or control to make sure compliance all the way down supply chain. Mr. Martin: we did an audit in 2014, 2017. Concern is how NASA is structured, people who sit in CIO position don't have full insights on all the systems or full control over IT spin, particular in mission systems. Mr. Seaton: that's been changing, I sit on other councils so I have full insights. There is collaboration with missions to make sure their systems are secure.
19. Rep. Babin: How many intrusions attempts last year? How does that compare to COVID? Mr. Seaton: measurements fluctuate, some increase because we have more visibility to know who's on the network.