IBM Newsroom

IBM To Establish New Cybersecurity Center For US Federal Clients

IBM Center for Government Cybersecurity to help agencies navigate current and future threats

Convenes advisory group of former government officials for expanded expertise

WASHINGTON, June 2, 2021 /PRNewswire/ -- IBM (NYSE: IBM) today announced that it is creating the IBM Center for Government Cybersecurity, a collaborative environment focused on helping federal agencies address current and future cybersecurity threats. The center will facilitate events and learnings, drawing on IBM's cybersecurity expertise from delivering software and managed services to over 17,500 security customers globally. Working with a group of internal IBM experts and external advisors, including former government officials with decades of cybersecurity experience, the center will leverage IBM technology and host workshops focused on priorities such as zero trust frameworks and cloud security, complemented by access to IBM Research labs to collaborate around the future of encryption.

As recent threats like SolarWinds and the Colonial Pipeline ransomware attack against critical infrastructure have shown, the threat landscape has crossed over from the digital world to the physical. In fact, the 2021 IBM Security X-Force Threat Intelligence Index found that ransomware accounted for 33% of the attacks on government organizations in 2020. With the US Federal government furthering its investment in hybrid cloud, new approaches for cybersecurity should focus on protecting both systems as well as data - no matter where it is – either on premise, in the cloud, or at the edge.

The IBM Center for Government Cybersecurity will be housed at IBM's offices in downtown Washington DC. The new facility will feature secured laboratory space where government customers can collaborate on unique solutions for advanced security threats leveraging insights from demos of IBM technologies and services. Initially, IBM will conduct virtual sessions to accommodate any challenges to meeting in person, with the capability to execute engagements at on-site customer locations.

"IBM is committed to helping our US Federal government customers meet cybersecurity modernization requirements – both for current and future threats," said Stephen LaFleche, General Manager Public and Federal Market, IBM. "Hybrid cloud environments can provide an opportunity to implement new technologies and techniques, like a zero trust framework and advanced encryption – while helping make the government more accessible and easier for citizens work with. These techniques are also being applied in other highly regulated industries, such as financial services, telecommunications and healthcare."

Center Exploring Current and Future Threats

A central goal of the IBM Center for Government Cybersecurity is to provide access to information on cybersecurity technologies IBM is using with the public and private sectors, and security innovations being developed in IBM Research laboratories via workshops. Some of initial examples of the sessions IBM will conduct include:

- **Adapting to a Zero Trust World** – Exploring the unique implementation needs for government to apply

the core principles of zero trust: least privilege access; never trust, always verify; and assume breach. IBM will leverage blueprints from successful public and private sector implementations to assist agencies to plan their zero trust journey. The session will explore four initiatives including: Securing the hybrid and remote workforce, Reducing the risk of insider threats, Protecting the hybrid cloud and Preserving customer privacy. As part of the center, IBM can demonstrate the capabilities of IBM Cloud Pak for Security to help orchestrate zero trust approaches. Customers can also experience the IBM Zero Trust Acceleration workshop to help manage new emerging requirements for a zero trust approach at US Federal agencies – with added expertise via partnerships like Zscaler and Illumio.

- **Hybrid Cloud Security Challenges for Data Portability** – Part of adapting zero trust models is disrupting the architecture design for IT systems. Agencies using multi-cloud and multi-tenant environments may be looking to securely modernize their applications and move data between on premise and cloud environments. As part of this workshop, IBM Security architects can demonstrate the use of trusted execution environments, containers, and open standards as a reference point for future hybrid cloud designs via IBM Security Services for Cloud. IBM is also helping customers protect data across hybrid environments for current threats. For example, IBM services and technologies are designed to maintain the highest available level of cryptographic key encryption protection to help protect existing data in the cloud[1] and prepare for future threats that could evolve with advances in quantum computing.

- **The Future of Cryptography** – With modern day cryptographic techniques threatened by advancements in computing, IBM Research is expanding its efforts in hardening this essential technology. IBM currently has several Quantum-safe cryptography standards in consideration with NIST and is at the forefront of making data usable while encrypted via Fully Homomorphic Encryption (FHE) and Confidential Computing. As part of this workshop, IBM researchers can help US Federal agency teams understand the implications that the technology will have on next-generation architectures and security protocols. IBM Z helps agencies protect against, and respond to threats, with technologies such as: encryption everywhere for data at rest and in transit to protect against data loss or corruption.

Expertise Available via IBM Center

The IBM Center for Government Cybersecurity Advisory Group brings together former public sector leaders and private sector experts that can advise US Federal customers on historical challenges and help evaluate best practices for navigating current and future regulations and orders. Access to the advisory group will be made available via on-site and virtual conferences as well as individual discussions. The Center Advisory Group will also publish thought leadership and research on cybersecurity issues and solutions.

Advisory group members include:

- Tony Scott - Former US Chief Information Officer
- Curt Dukes - Former Information Security/Cyber Security Lead for NSA
- Kiersten Todt - Former Cybersecurity Advisor for President Obama
- Margaret Graves - Former Deputy Federal CIO and Deputy DHS CIO
- Daniel Chenok - Former Branch Chief for OMB
- Brian Dravis, Major General (ret) - Former Director Joint Service Provider DISA, DOD

- Terry Halvorsen - Former DOD CIO, DON CIO, and Deputy Commander Network Warfare Command

The world-renowned IBM Security X-Force research organization will also be available via Center events. IBM Security X-Force monitors 150 billion+ security events per day in more than 130 countries. Early access to research from X-Force will be available for US Federal customers engaged via the Center.

US Federal agency customers seeking more information on the IBM Center for Government Cybersecurity should speak to their IBM representative or visit: http://ibm.biz/us-federal-cyber-center

About IBM Security
IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM Security X-Force research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 150 billion+ security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. IBM Security offers a completely flexible deployment model from consultancy, advice from industry experts, advanced technology to managed security services. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

Media Contact:
Michael Rowinski
IBM External Relations
rowinski@us.ibm.com

[1] Encryption keys and cryptographic operations are protected with highest level certified HSM - with Hyper Protect Crypto services: FIPS 140-2 Level 4.

SOURCE IBM
