NATIONAL INSIDER THREAT TASK FORCE (NITTF)

Greetings,

The Enterprise Threat Mitigation Directorate (ETD) and the National Insider Threat Task Force (NITTF) is sponsoring a virtual community forum, called **Enterprise Threat Discussions,** on **November 16th, 2021, from 10:00 AM to 11:00 AM** on the topic of **Zero Trust.**

Dates/Location: November 16, 2021 (Tuesday) from 10:00 AM to 11:00 AM EST, virtually on WEBEX by invitation only.

GUEST SPEAKER: Sean Connelly - Trusted Internet Connections (TIC) Program Manager, CISA, DHS

Please forward this notice to individuals with defensive CI, insider threat, or security roles in your organization who might benefit from knowing more about the Zero Trust security model. If interested, they should provide their name, position title/role, and email address to **Brittany Wheeler at brittany.c.wheeler@odni.gov**. Once we have their registration information, we will send them a Webex Link. If you have any questions, please let us know.

Topic Summary:

This episode will provide an unclassified overview on the Zero Trust security model. Zero Trust is a set of system design principles, and a blended cybersecurity and system management strategy based on the understanding that threats exist within and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any single element, service or node and instead requires continuous verification and validation. The purpose is to ensure that all users and components have the right privileges and attributes to access vital network resources. The principle of least privileged access is one of the core tenets of Zero Trust mean which means all users should have the absolute minimum permission needed to carry out their work function and nothing more. To mitigate the growing risk of insider threat activity, many organizations are turning to a Zero Trust model that helps to better modernize security inside and outside the network perimeter with continuous verification of user access.

Speaker Bio:

The briefing will be presented by Sean Connelly who serves as the Trusted Internet Connections (TIC) Program Manager at the Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS). In this role, he leads the TIC Program Management Office, which is responsible for leading the Office of Management and Budget's TIC initiative within CISA. The TIC initiative is the federal government's strategy to securely protect government networks that connect to the Internet and cloud providers. CISA's TIC Program Office works with a wide-spectrum of partners across government and industry and leads the way at enhancing network security across the federal enterprise horizon.

Mr. Connelly joined DHS in 2013 and has served in a variety of roles, including the development of TIC 1, 2 and 3, along with the deployment of CISA's sensor capabilities (operationally known as EINSTEIN 3A), and was part of the initial architectural team that stood-up the Continuous Diagnostics and Mitigation program. Additionally, Mr. Connelly was a lead author on the 'IT Modernization Report to the President' in 2017, as well as a co-author of NIST's Special Publication towards 'Zero Trust Architectures' in 2019.

Prior to joining the federal civilian service, Mr. Connelly worked as a consultant to the Department of State, where he led architectural initiatives within the department, including the adoption of TIC 1 and TIC 2, as well as the design of the State Department's next-generation telecommunications platform, providing IT for a global workforce. Overall, Mr. Connelly has over 15 years of experience in the federal domain, and over 20 years of experience in the IT and cybersecurity domain.

Mr. Connelly earned a MS in Information Technology Management from George Washington University, and holds two Cisco Certified Information Expert (CCIE) certifications. Mr. Connelly holds the first CCIE in Routing, and a second CCIE in Security.