Connection
PUBLIC SECTOR SOLUTIONS
we solve IT

COMPLY TO CONNECT (C2C)

Securing the Outcomes of Government IT

Multiple breaches have occurred against Federal Government and Department of Defense (DOD) institutions. Data breaches continue to increase and are expected to reach an all-time high in this year. Are you prepared?

New DOD Cybersecurity Regulations Are Here

The cybersecurity challenges facing federal government agencies are more complex than ever before. The federal government has recognized the need to increase cybersecurity protection, detection, and response. This requires tools to ensure trusted users and authorized device are rigorously inspected for malicious code, prohibited software, noncompliance, human error, and other risks.

On May 12, 2021 the Biden Administration issued an Executive Order on Improving the Nation's Cybersecurity. The order states, "Incremental improvements will not give us the security we need; instead, the federal government needs to make bold changes and significant investments to defend the vital institutions that underpin the American way of life."[1] Additionally the policy states, "The federal government must adopt security best practices; advance toward Zero Trust architecture; accelerate movement to secure cloud services and invest in both technology and personnel to match these modernization goals."[2] This makes it clear that the federal government recognizes the immense risk faced with protecting the confidentiality, integrity, and availability of wide-ranging applications, services, and data.

Connection Can Help

Earlier this year, a supporting DOD memorandum mandated compliance with Comply2Connect. C2C is a logical first step on the pathway Zero Trust, and Connection has you covered. We have demonstrated proven success in implementing C2C within the

1,2 United States, Executive Office of the President [Joseph Biden]. Executive Order 14028: Improving the Nation's Cybersecurity, May 12, 2021.

DOD—successfully rolling out C2C programs, including the integration and operational turn-up of hundreds of DOD sites, to achieve the following steps that are critical to cybersecurity:

- Authenticating and authorizing the endpoint
- Policy-based authentication
- Endpoint reporting and publishing to the DOD Enterprise Endpoint Repository
- Appropriately authorizing assets to network segments, regardless of user
- Continuously monitoring authorized device activities through the orchestration and integration of detection and validation tools

Connection's highly trained and certified engineers are your secret to success in meeting all your C2C directives. Implementing C2C is a massive, sprawling initiative with many moving parts. When you're ready, the Connection team is here to guide you through the process. You don't have to go it alone. We've got the experience and expertise to help your organization succeed.

The Technology Partner to the Federal Government

With more than 25 years of service to the federal government, Connection is the proven, premier partner you need for procuring mission-critical IT solutions. Ensure your organization is supported with a modern, optimized C2C framework and the technologies necessary to make cybersecurity more effective and efficient across your network.

Connection®
PUBLIC SECTOR SOLUTIONS
we solve IT®

Contact a Connection Expert Today.

1.800.800.0019
www.connection.com/ps