GENERAL DYNAMICS
Mission Systems

COMPLIANCE WITH BIDEN MEMORANDUM

OVERVIEW

On January 19, 2022, President Biden signed a National Security Memorandum (NSM) to outline specific actions agencies need to employ to ensure all National Security Systems (NSS) use the same network cybersecurity measures of federal civilian networks per the largely overlooked Executive Order 14028, Improving the Nation's Cybersecurity.

Executive Order 14028 establishes that the Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to malicious cyber campaigns and their actors through bold changes and significant investments in cybersecurity.

EXECUTIVE ORDER 14028

The importance of this NSM cannot be overlooked as today's dynamic cyber landscape presents a significant challenge for those charged with protecting sensitive data and defending National Security, Department of Defense and Intelligence Community systems. Sharing and communicating this data across a landscape mired by varying physical locations and diverse digital domains is made more complex by its exponential growth and increasing importance.

4 CORE TENETS

- The government "shall adopt National Security Systems requirements that are equivalent to or exceed the cybersecurity requirements set forth in this order."
- Requires agencies to identify their national security systems and report cyber incidents that occur on them to the National Security Agency, which by prior policy is the "National Manager" for the U.S. government's classified systems.
- NSA to create Binding Operational Directives requiring agencies to take specific actions against known or suspected cybersecurity threats and vulnerabilities.
- Requires agencies to secure cross domain solutions – tools that transfer data between classified and unclassified systems.

While these priorities are not new, this NSM brings them to the forefront again to help accelerate the adoption and implementation of the outlined cybersecurity requirements. It is paramount that agencies understand the significant importance of these directives and prioritize the steps that need to be taken to modernize cybersecurity defenses and build resiliency in short order.

These requirements will now be more strictly enforced by the Executive Branch, and at General Dynamics Mission Systems, we understand that our customers are pained by continually ensuring their services meet pertinent policies, regulations and accreditations. And gone are the days of “special cases” that historically allowed agencies to circumvent certain requirements. Now, agencies are obligated to abide by all requirements – our national security depends on it.

Fortunately, General Dynamics Mission Systems is ahead of the curve and has been meeting these security standards long before the NSM’s release. General Dynamics knows that every piece of data is critical to our national security. Always innovating in partnership with customers, we have proactively invested in research, technologies and forward-leaning approaches to reduce risk and cost, and shorten certification and accreditation timelines, shifting what we can away from the mission.

Our products protect all forms of data including data in transit, data at rest, and data traversing across all domains from the enterprise to the tactical edge. No matter the journey, we secure Top-Secret and Below data wherever it may travel.

Clients using our products do not have to worry about becoming compliant with this NSM — they already are. And those exploring solutions can have the confidence that our products will help them not only come into compliance but be prepared for evolving requirements with products designed with the future in mind.

Confidence in Your Digital World™

GOING BEYOND COMPLIANCE NOW

General Dynamics Mission Systems' products are designed to address the imperatives laid out in this NSM and are ready to deliver now to protect and defend all military and federal networks. Data protection across the network is what secures the network. From the depths of the ocean to the beyond of space, our products protect data as it:

- hops from a mobile office to a classified system
- is collected during unmanned operations
- falls into the hands of our adversaries or left behind
- flies through the friendly (and not so friendly) skies
- crosses medians spanning thousands of miles
- is shared and transmitted across different networks or enclaves and varying security levels in austere tactical environments
- uplinks and downlinks from here to all regions in space
- hand carried or soldier mounted

RAISE THE BAR COMPLIANT

tactical cross domain solutions

NSA CERTIFIED

high assurance type 1 encryption products

NSA CERTIFIED HIGH ASSURANCE TYPE 1 ENCRYPTION PRODUCTS

Our NSA certified high assurance Type 1 encryption products for data in transit and data at rest can help agencies meet cybersecurity requirements protecting classified information and NSS, as they are developed using established and stringent NSA processes and integrates NSA approved cryptographic algorithms and multifactor authentication. While commonly assumed high assurance Type 1 and Commercial Solutions for Classified (CSfC) products are interchangeable, CSfC products have reduced development time, handling and testing requirements. Therefore, per NSA doctrine, organizations that decide to implement CSfC solutions must accept that they, the end user, must assume and accept the risks associated with the CSfC solution implementation. Whereas the use of NSA certified Type products recognizes and validates that each product has been rigorously and successfully tested and verified to meet all applicable security and interoperability standards in a wide variety of applications and environments.

System integration can be cumbersome, time-consuming, and expensive. Our data at rest and data in transit encryption products comply with standards-based cryptographic communication protocols to enable ease of integration of individual components into larger systems. At General Dynamics Mission Systems, our design teams have taken the time to meet standards and test them for compliance, so by the time our customers get the devices in their hands, they work seamlessly in their larger systems.

General Dynamics Mission Systems’ design teams also account for unique mission protocols, and for decades we have implemented crypto mod initiatives for secure voice and data information assurance. Our products are designed with crypto modernization in mind and are being designed for future crypto mod requirements. This protects the customer’s investment as hardware upgrades and modernization efforts can be performed in the field with minimal impact to the mission.

> “ **Our reason for being at General Dynamics Mission Systems is to make sure that our customers and the national security establishment have the most secure crypto that American ingenuity can provide.**
>
> BRIAN MORRISON, BREAKING DEFENSE

To help customers plan for mission needs, General Dynamics designed, developed and implemented features to add enhanced capabilities.

- **Advanced Cryptographic Capabilities (ACC)** modernizes cryptographic algorithms to defend against modern and advanced cyber threats. This upgrade is easily field upgradeable and is backwards compatible with earlier releases.
- **Key Management Infrastructure (KMI) Over-the-Network Keying (OTNK)** improves key management for faster, simpler, safer operations by enabling automatic and immediate key generation and delivery for HAIPE devices.
- **Agile Virtual Local Area Network (VLAN)** adds bandwidth-efficient Layer 2 encryption to HAIPE encryptors and helps facilitate the flexible deployment of secure networks.
- **Heartbeat Signal Zeroize** for high risk and unmanned environments requires signals to be received at regular intervals or, if lost, zeroized is triggered rendering the system useless.
- **Render Useless Zeroize (RUZ)** provides a fast, simple way to make the TACLANE inoperable and inaccessible so adversaries cannot access information or equipment by eliminating Critical Security Parameters like cryptographic keys and algorithms.
- **TACLANE® Trusted Sensor Software** adds IDS/IPS capabilities to aid network administrators in establishing network situational awareness and provides greater Defense-in-Depth in a cost-effective manner.
- **Agile Performance Enhancing Proxy (PEP)** uniquely provides accelerated performance in disadvantaged networks, as well as simultaneous support for concurrent TACLANE Agile PEP, Standard TCP connections and all HAIPE traffic types on a per packet basis.

TACLANE

With its first introduction in 2000, TACLANE is the world's most widely deployed Type 1 encryptor for good reason.

- **TACLANE-C175N CHVP Encryptor** bridges high assurance Type 1 certified security & interoperability with COTS handling and end user devices.
- **TACLANE-1G (KG-175G)** is a smaller, more power efficient 1 Gb/s high-speed encryptor, ruggedized for both tactical and strategic environments.
- The **TACLANE-10G (KG-175X)** is the only ACC compliant 10Gb HAIPE encryptor, providing end-to-end 20 Gb/s throughput speed and offers simultaneous IP and Ethernet capabilities.
- **TACLANE-Nano (KG-175N)** approaches 200 Mb/s aggregate throughput to provide the high bandwidth needed in the smallest, lightest and lowest power configuration available today and is a modern replacement for legacy fast Ethernet encryptors.
- The **TACLANE-FLEX (KG-175F)** is scalable to support 200 Mb/s to 2 Gb/s aggregate throughput and offers greater control over the device's power consumption for increased power efficiency and decreased operating and touch temperatures and related lifecycle costs.

To address the requirement for high bandwidth encryption supporting the low latency, security and performance requirements of high speed layer 2 network backbones, the introduction of the TACLANE E-Series Ethernet Data Encryption Cryptographic Interoperability Specification (EDE-CIS) compliant product family expands our market-leading encryption capability to a new set of agencies and missions.

Some missions do not require the high level of security and handling as Type 1 CCI products. And as an alternative to limited CSfC solutions, we recently introduced the TACLANE-C175N CHVP encryptor for which we expect NSA certification imminently.

GEM® One enables administrators to visualize and manage a network of dispersed encryption devices — including their health, status and connectivity – from anywhere in the network or remote login.

	TACLANE-C175N	TACLANE-Nano KG-175N	TACLANE-Micro KG-175D	TACLANE-FLEX KG-175F	TACLANE-1G KG-175G	TACLANE-10G KG-175X	TACLANE-ES10 KG-185A	Sectéra® vIPer™
ACC & KMI OTNK Compliant	✓	✓	✓	✓	✓	✓	✓	ACC
Agile VLAN Capable	✓	✓	✓	✓	✓	✓	Supports VLAN Tagging	
Render Useless Zeroize (RUZ)	✓	✓		Planned			✓	
Cyber Sensing Capable with TACLANE Trusted Sensor (TTS)				✓	✓	✓	N/A	
TCP/IP Performance Enhancing Proxy (PEP) for SATCOM HAIPE	✓	✓		✓			N/A	
GEM ONE Management	✓	✓	✓	✓	✓	✓	✓	✓

PROTECD@R®

General Dynamics family of ProtecD@R high assurance Type 1 encryption products protect our Nation's most sensitive data at rest, designed for both enterprise and tactical environments.

The high assurance ProtecD@R Multi-Platform (KG-204) is the only operating system and host-agnostic data at rest encryptor approved for unmanned systems.

Special missions require special technologies to protect certain data at rest. We build custom solutions tailored to specific needs so customers get what they need in a certified product, meeting compliance requirements.

SECTÉRA vIPer UNIVERSAL SECURE PHONE

The Sectéra vIPer Universal Secure Phone, the only NSA certified universal secure phone, allows you to easily switch between making end-to-end secure and non-secure calls on Voice over IP and analog networks. Enclosed inside the Iridium 9575A handset, the Sectéra Iridium Security Module 2 (ISM2) is a sleek, small form factor encryption module that provides SA certified protection.

ADVANCED INFOSEC MACHINE (AIM) III

Advanced INFOSEC Machine (AIM) III chip is a programmable, embeddable security engine for communications equipment requiring high-grade cryptographic processing. This next-generation version builds upon 50 years of fielded high assurance cryptographic chips, modules and communication products. AIM III, delivering higher performance and using less power in a smaller footprint, can reuse prior cryptographic applications with minimal modifications for faster execution.

KOV-28 OPEN SYSTEMS ARCHITECTURE (OSA)

Our NSA certified KOV-28 Open Systems Architecture (OSA) crypto module is built with standards specific to rugged military applications and secures communication channels across contested environments on a variety of platforms. The flexible OSA design allows for upgrades and modifications as quickly as the threat environment demands.

To bring new innovation to and drive capabilities into our products, we are persistent in our pursuit as we peer into the future to identify technologies that we can pull forward. General Dynamics has and is investing in Zero Trust architectures and how the application of "never trust, always verify" can help improve and strengthen how our products secure networks.

Our TACLANE products seamlessly integrate with existing Zero Trust Architecture authentication services, including 802.1x — an authentication standard for device network access control on wired and wireless access points.

Our ProtecD@R data at rest encryptors permit devices that support Zero Trust architecture as our products provide transparent security capabilities between the host and the drive.

truMLS®

truMLS is an open platform solution that eliminates the need for multiple networks, applications, and endpoints at varying security and access levels. It leverages Zero Trust principles:

- **Dynamic and Mandatory Access Control (MAC)** of data, objects and resources.
- **Secure operating system** architected for multilevel certification and accreditation.
- **Immutable data label option** to enforce provenance of data source.
- Data in transit **tagged with security classification label**.

General Dynamics utilizes a rigorous, complicated and demanding Continuous Certification Process to maintain high assurance and keep re-certifications current. The resulting decreased costs and shortened schedule directly benefits customers by keeping them in compliance with the continued efforts of strengthening our Nation's cybersecurity and modernizing defenses.

RAISE THE BAR COMPLIANT TACTICAL CROSS DOMAIN SOLUTIONS

TACDS®

The General Dynamics Raise the Bar compliant Tactical Cross Domain Solution (TACDS) stands above the rest. Designed to enable trusted information sharing across agencies and with coalition partners across different security domains, TACDS provides instant, secure access to real-time information for warfighters serving on the modern joint and all-domain battlefield of today.

- ✓ Meets NSA's Phase 1 Raise the Bar Requirements
- ✓ Lowest SWaP-C Tactical Hardware CDS in Production Today
- ✓ Secret and Below Interoperability (SABI) Certified
- ✓ Supports Dozens of Tactical Message Formats

TACDS FILTER LIBRARY

RAISE THE BAR COMPLIANT	HD Full Motion Video with KLV metadata	Configurable XML	Configurable Protobuf	Configurable Binary	MIL-STD 6017 -/A/B/C VMF
STANAG 4586 Payload/ Platform Control	USMTF	SNMP	ICMP	MISD-C2	MIL-STD 6016 Link 16/ MIL-STD 3011 JREAP-C
UTAMS	TLS/SSL	FTP	SMTP	FDMP	PNC

APPLICATIONS

TACDS supports a wide variety of tactical deployments and systems. TACDS can process numerous mission-enabling tactical data and message formats to provide instant, secure access to real-time information for warfighters serving in today's tactical environment. **With its broad capabilities, TACDS is specifically designed for diverse applications on the modern battlefield, including:**

- **Situational Awareness (SA) and Command & Control (C2):** Variable Message Format (VMF) Messages; SA & C2 Data; Position/Location Information (PLI); MEDEVAC
- **Real-Time Condition Based Maintenance:** Vehicle Health & Status Monitoring; Remote Maintenance & Vehicle Diagnostics; Fuel & Ammunition Level Monitoring
- **Coalition Interoperability:** STANAG 4677; Realtime SA & C2; ISR Video Collaboration
- **Real-Time ISR Data Collection & Dissemination:** Unmanned Aerial Vehicle (UAV) Video; Unmanned Ground Sensors; Remote Sensor Video; Every Soldier as a Sensor; Vehicle-mounted Cameras; Soldier-carried Cameras
- **Unmanned Vehicle Control:** STANAG 4586 — UAV Platform and Payload Control; Cursor on Target (COT); STANAG 3277 — Air Reconnaissance; Text Based Sensor Cueing Messages

Information sharing in support of national security missions needs to be secure at a level mandated by the U.S. government because it is that important. NSA's National Cross Domain Strategy & Management Office (NCDSMO) serves as the lead entity responsible for overseeing these cross domain activities. Raise the Bar establishes architecture, design, development, engineering, implementation, system security, local and remote management and monitoring, and filtering standards and guidelines to ensure that these systems are secure and meet the cybersecurity requirements set forth in the NSM.

Today TACDS is available in two form factors: the TACDS-Vehicle Mount (VM) and TACDS-Low Profile (LP). Both meet Phase 1 Raise the Bar stringent requirements set forth by NSA that establishes security guidelines and requirements for cross domain solutions deployed by U.S. government to protect NSS data. TACDS executes programmable rule sets that filter information, allowing individual messages or data fields within them to be selectively passed, blocked or changed. This innovative method ensures data security on both networks and automates the "man in the middle" screening of message exchanges to accelerate communications and reduce human errors.

Exceptions can only put these systems at risk. With TACDS, agencies can avoid unnecessary exposure and quickly come into compliance with established cybersecurity requirements.

BE COMPLIANT NOW AND BE PREPARED FOR WHAT'S NEXT

Our continuous product research and investment based on direct and ongoing customer collaboration has allowed General Dynamics to bring effective, compliant, accredited products to the market and the mission. We do the hard work, so agencies focus on the protection of sensitive data and defense of National Security, Department of Defense and Intelligence Community systems in a topography that is constantly shifting and reacting to outside forces.

We continue to build on our track record by expanding our offerings and introducing new products and capabilities that keep our customers compliant with federal regulations and responsive to imminent threats both now and in the long-term. We never forget that our adversaries will target the weakest link and we bring every resource to bear to build products that strengthen every link in our Nation's cybersecurity chain.

Our experience and expertise can help agencies immediately address these critical data protection requirements today. There is only one thing more important than data protection — protecting our Nation and its people.

THE URGENCY IS REAL.