IRON BOW® TECHNOLOGIES

From Risk Management to Agile Security

Aligning BOD 2024-02 to Post Quantum Cryptography



© Iron Bow Technologies. All rights reserved.

Table of Contents

Executive Summary 3

What Does This Mean for Me? 4

Commercial Solutions for Classified (CSfC): An Additional Pathway to CNSA 2.0 Readiness 6

Practical Strategies: From BOD Compliance to Quantum-Safe Architectures 8

The Bottom Line 9



Executive Summary

Short-term, compliance-based cybersecurity practices cannot adequately protect against evolving modern threats. Cybersecurity and Infrastructure Security Agency (CISA's) Binding Operational Directive (BOD) 2024-02 represents an important step in strengthening classified communications by introducing additional commercial encryption protections alongside existing Type 1 encryption devices. While these measures address immediate security concerns and strengthen today's classified transport architectures, emerging threats such as quantum computing require organizations to consider how these protections will evolve over time.

To protect against these emerging threats, National Security Memorandum -10 (NSM-10 in 2022) and Executive Order (EO14144) have mandated organizations to pivot towards the new Commercial National Security Algorithm Suite 2.0 (CNSA 2.0). By planning for CNSA 2.0 adoption and selecting cryptographically agile technologies, agencies can reduce future cryptographic risks while preserving the ability to adapt their security architectures as approved post-quantum capabilities become available.

Agencies preparing for the transition to CNSA 2.0 should evaluate modernization opportunities across both existing Type 1 encryption infrastructures and NSA's Commercial Solutions for Classified (CSfC) program. BOD-aligned architectures provide an opportunity to strengthen transmission security through commercial encryption technologies, while CSfC presents a compelling alternative for organizations seeking greater architectural flexibility, commercial technology integration, and cryptographic agility. Both approaches can support a phased transition toward quantum-resistant security capabilities, allowing agencies to address immediate operational risks while preparing for future cryptographic requirements.

THE KEY TAKEAWAY

Organizations should not treat BOD 2024-02, CSfC, and CNSA 2.0 as competing initiatives. Instead, they represent complementary opportunities to strengthen today's classified transport architectures, introduce cryptographic agility, and prepare for future post-quantum security requirements.

What Does This Mean for Me?

CNSA 2.0 is more than a cryptographic update; it represents a modernization requirement that will influence procurement, system design, and lifecycle management decisions across National Security Systems (NSS). Organizations must consider how today's classified transport architectures can evolve to address emerging quantum threats while maintaining operational security and protecting existing investments.

BOD 2024-02 and CNSA 2.0 address complementary security objectives:

- **BOD 2024-02 — Strengthening Today's Defenses:** Reinforces existing Type 1 encryption architectures through additional commercial transport encryption protections, helping address immediate operational security concerns and improve TRANSEC capabilities.
- **CNSA 2.0 — Preparing for Tomorrow's Threats:** Establishes the direction for quantum-resistant cryptography, protecting sensitive information against future cryptographically relevant quantum computers (CRQC).

Two Architectural Modernization Pathways

As organizations prepare for CNSA 2.0, two approaches should be considered:

Path A

Modernize Existing Type 1 Architectures

Preserve TACLANE investments while evolving the transport encryption layer with cryptographic agility and post-quantum capabilities as supported. This approach strengthens the existing architecture without requiring wholesale replacement.

Path B

Adopt CSfC Architecture

Evaluate NSA's Commercial Solutions for Classified (CSfC) program as an alternative that uses two independent layers of approved commercial encryption. CSfC offers flexibility in technology selection, deployment, and lifecycle modernization, providing a potential pathway toward PQC readiness.

Both approaches can contribute to a long-term cryptographic modernization strategy. The appropriate selection depends on mission requirements, existing infrastructure, operational constraints, and the availability of approved cryptographic technologies. **BOD strengthens today's classified transport architecture. CNSA 2.0 creates the opportunity to modernize it.** Organizations have two architectural pathways to consider.

For example, BOD 2024-02 highlights how network fingerprinting and data exposure are prime targets today, while CNSA 2.0 ensures that future cryptographic protections can help safeguard intercepted data against quantum-enabled decryption. Together, they reflect a broader shift in federal cybersecurity toward continuous risk reduction across both present and emerging threats.

As agencies prepare for CNSA 2.0, two modernization pathways emerge: strengthening existing Type 1/TACLANE architectures through evolving transport encryption capabilities or adopting NSA's Commercial Solutions for Classified (CSfC) framework as an alternative layered encryption architecture. Both approaches offer opportunities to incorporate cryptographic agility and prepare for post-quantum capabilities as approved technologies become available.





Commercial Solutions for Classified (CSfC): An Additional Pathway to CNSA 2.0 Readiness

The CSfC is a program run by the National Security Agency (NSA) that allows government and approved trusted integrators to protect classified information using commercial off-the-shelf (COTS) technology instead of only traditional Government of the-Shelf (GOTS), purpose-built encryption systems.

At its core, CSfC is based on a layered security concept. Rather than relying on a single, highly specialized encryption device, it uses two independent layers of encryption (often called “dual layer” or “layered encryption”) built from vetted commercial products. These layers must follow strict architectures defined by NSA, ensuring that even if one layer were compromised, the data would remain protected. CSfC also establishes strict requirements for maintaining independence between encryption layers, including separation of administrative responsibilities and compliance with applicable Capability Package requirements. This approach enables insights and visibility into secure solutions for transmitting and storing classified data, up to Top Secret, over COTS infrastructure.

CSfC can accelerate deployment and provide cost advantages for certain mission requirements. Agencies can leverage widely available commercial technologies, while still meeting national security requirements. It also increases flexibility, allowing classified capabilities to be extended to mobile users, remote locations, embassies, and coalition environments through approved architectures tailored to operational needs.

By leveraging secure, standardized commercial technologies, CSfC provides an alternative approach to protecting classified information by addressing immediate cybersecurity mandates like BOD 2024-02 and supporting long-term cryptographic modernization objectives under CNSA 2.0.

For BOD 2024-02, which focuses on responding to active threats (especially around networking fingerprinting and data exposure), CSfC can provide an alternative architecture that strengthens defenses through its layered encryption and commercial security stack. CSfC architecture can integrate secure identity management, strong authentication (including MFA), encrypted communications, and continuous monitoring. This directly supports BOD priorities like protecting sensitive data in transit, reducing the risk of credential misuse, and limiting the impact of breaches. Because CSfC solutions are built from widely available commercial technologies, they can offer deployment flexibility, aligning with the directive's emphasis on rapid risk mitigation.

For CNSA 2.0, CSfC provides a pathway to adopt and integrate quantum-resistant cryptography over time. Since CSfC is based on modular commercial components (VPNs, encryption tools, endpoint devices), organizations can plan incremental cryptographic upgrades as approved post-quantum capabilities become available within supported commercial components and NSA Capability Package requirements. Its dual-layer encryption model also aligns well with cryptographic agility objectives by allowing organizations to evaluate modernization opportunities across independent encryption layers. This makes CSfC a practical way to modernize without needing to completely rebuild systems.

Taken together, CSfC provides a compelling pathway toward future transmission security needs by enabling flexible, layered architectures and opportunities for phased cryptographic modernization. At the same time, organizations with established Type 1 encryption infrastructures can strengthen their existing BOD-aligned architectures by incorporating evolving post-quantum capabilities into their transport encryption layer. Both approaches support operational security today while providing opportunities to build cryptographic agility and prepare for CNSA 2.0 requirements tomorrow.

Practical Strategies: From BOD Compliance to Quantum-Safe Architectures

Stabilize and Comply (short term)

First, fully meet BOD 2024-02 requirements:

- Identify impacted systems and data
- Reset/secure identities and credentials
- Enforce strong outer layer of encryption and monitoring

Closing active gaps quickly, don't try to redesign architecture yet.

Map BOD Controls to Future Security Capabilities

Next, translate what you implemented into long-term security capabilities:

- Data protection → layered encryption and cryptographic agility
- Monitoring → continuous diagnostics within the encryption architecture

Build upon existing BOD protections as part of a long-term modernization strategy.

Evaluate Type 1 and CSfC Architectures

Evaluate the appropriate architecture for your mission:

- Modernize existing Type 1/TACLANE infrastructure through enhanced transport encryption
- Consider CSfC architectures with two independent commercial encryption layers
- Assess operational requirements, existing investments, and long-term crypto agility

Select the architecture that best supports mission requirements, existing investments, and future cryptographic agility.

Pilot and Phase In

Pilot the selected modernization architecture, including CSfC registration where applicable:

- Migrate or upgrade a subset of users, systems, or transport connections
- Validate performance, usability, and security controls
- Scale CSfC pilot out to Enterprise Scale the validated architecture across the enterprise

Validate the selected architecture before expanding deployment across the enterprise.

Integrate Identity and Zero Trust Principles

Layered security architectures can reinforce broader Zero Trust objectives:

- Strong identity binding across layers encryption components
- Continuous authentication and device validation
- Integration with Zero Trust Architecture

Reinforce identity, authentication, and continuous monitoring across the security architecture.

Plan for CNSA 2.0 Alignment

As you expand CSfC modernize your encryption architecture:

- Select products with post-quantum (or PQC-ready) roadmaps
- Prepare for possible hybrid cryptography inside CSfC layers where supported by approved implementations
- Build crypto agility into procurement

Ensure the modernization strategy supports CNSA 2.0 transition requirements and timelines.

The Bottom Line

The transition to post-quantum cryptography presents an opportunity to strengthen existing classified transport architectures while preparing for emerging threats. **Whether organizations continue modernizing their Type 1 encryption infrastructure or adopt CSfC-based solutions, the objective remains the same: reduce today's operational risks while building cryptographic agility for tomorrow's requirements.**

Aligning BOD-driven security improvements with CNSA 2.0 transition planning, agencies can make informed architectural decisions that preserve existing investments, support mission requirements, and establish a foundation for long-term cryptographic resilience. Applying the scalable, standardized framework of CSfC enables organizations to reduce the risk of today's threats, while building a flexible architecture to reduce the risk of future ones.

The goal isn't to replace one with the other, but to build upon today's security requirements through a sustainable modernization strategy. Whether strengthening TACLANE-based architectures or adopting CSfC, organizations can leverage cryptographic agility to prepare for emerging threats and future requirements under CNSA 2.0.



IRON BOW® TECHNOLOGIES

Ready to enhance your classified data security and asset management?

Contact Iron Bow today to learn how we can help your organization achieve its CSfC goals at csfc@ironbow.com or ironbow.com/contact-us.



Iron Bow Technologies
2121 Cooperative Way, Suite 500, Herndon, VA 20171
703.279.3000 800.338.8866 | info@ironbow.com

© Iron Bow Technologies. All rights reserved.