The Growing Need to Protect Classified Data at Rest (DaR):

How high assurance encryption can meet your mission needs and reduce operational risk

January 2020, Updated October 2021

GENERAL DYNAMICS
Mission Systems

Contents

DATA AT REST IS DATA AT RISK

Today's national defense systems are capable of collecting and storing massive amounts of data at varying classification levels. In parallel, increasing cyber threats make this data is more susceptible than ever before to both external and internal attacks. Loss of classified data can put our Nation at risk by debilitating our warfighter's effectiveness, exposing internal infrastructures to attack, and revealing technological advantages to our adversaries. The privilege of handling classified data comes with the responsibility to protect it.

Historically, Department of Defense (DoD) cyber defenses have focused on protecting data as it travels across our networks (i.e. Data In Transit); however, that is only half of the solution. Data at Rest (DaR) (i.e. stored data) is also subject to cyber threats, as we have seen with the proliferation of data breaches over the past decade across the private and public sectors. This paper focuses on the options defense organizations have to protect their most sensitive DaR from insider threats and external attacks; solutions that make it easier than ever before to meet protection mandates and reduce operational risk.

Within enterprise environments, guns, gates and guards can no longer offer complete protection of classified data. Due to its high-value nature, classified DaR is prone to both inside and outside threats. On the front lines, the hazardous locations and operational mission parameters of today's combat and intelligence, surveillance and reconnaissance (ISR) platforms make them more susceptible to compromise or overrun while deployed. Data stored onboard these platforms can expose strategic and tactical intelligence and must be protected. High assurance encryption (known as NSA certified high assurance Type 1) has been, and continues to be the most robust way to safeguard classified information.

For years, complying with DaR security requirements has been a daunting task for DoD programs, as few high assurance options have existed which meet their cost, schedule and performance objectives. Waivers granted by an organization's Information Assurance (IA) official have allowed programs to proceed without the required security. Today, the increasing requirements to conform to the Federal Risk Management Framework (RMF) is driving organizations to look for permanent solutions that will truly protect DaR as governed by current policy.

The following are examples of existing Federal DaR policy:

Joint Chiefs of Staff
CJCSI 6510.01F: IA and Support to Computer Network Defense (CND)
"Protection of DaR: Classified national security information shall be protected using NSA-approved cryptographic… systems…approved for protecting classified information."

Department of Defense
DODI 8320.02: Sharing Data in the DoD
"Components must ensure all DoD information programs…will protect data in transit and DaR according to their confidentiality level, mission assurance category…"

U.S Army
Pamphlet 25-2-16: COMSEC
"Only NSA-approved cryptographic products… that have been endorsed by the CIO/G–6, Cybersecurity Directorate and listed in the Army ISSPA will be used for the protection of classified information."

Air Force
AF Manual 17-1301: COMPUSEC
"DaR and data in transit protection requires FIPS 140-2 validated cryptographic modules for securing CUI and PII and NSA approved cryptographic systems for classified data …"

National Institute of Standards and Technology (NIST)
SC-28: Protection of Information at Rest
"The strength of [cryptographic] mechanism is commensurate with the security category and/or classification of the information."

Table 1: Select Federal DAR Policy; see GDMissionSystems.com/DaRPolicy for complete list

> ***Organizations must determine the level of risk they are willing to accept when protecting classified DaR.***

In order to obtain the authority to operate (ATO), a DoD program's method for DaR protection must be approved by the organization's Authorizing Official (IA official). This approval indicates the amount of risk the organization is willing to accept. The following section addresses the various solutions available and their associated risks.

DaR PROTECTION OPTIONS

Due to limited insight into available DaR options these decisions are often made late in the program's development cycle, when the focus turns towards obtaining the ATO. This lack of awareness early on drives last minute decisions based on perceived cost and schedule impacts vs. the potential risk. Selecting a DaR security solution ought to occur early during security architecture designs, with a focus on safeguarding the systems stored data in the event of compromise.

Classified DaR encryption requirements can be addressed in one of three ways:

RISK	SOLUTION TYPE
High	**Commercial-Grade** Requires waiver from IA authority
Medium	**Commercial Solutions for Classified (CSfC)** Uses commercial components, requires IA authority approval
Low	**High Assurance (Type 1)** Certified by NSA, alleviates risk from performing organization

Commercial Encryption (High Risk)

The commercial encryption market is saturated with solutions from hardware like self-encrypting drives (SED), to various software file and full-disk encryption options. Regardless of the brand or strength of the encryption used (e.g. AES 256, FIPS 140-2) commercial encryption products may contain vulnerabilities that can expose the key or data. There are also supply chain risks to consider with hardware components manufactured by untrusted foreign suppliers.

Software-based encryption alone is not suitable for protecting classified data, as it is only as secure as the system running the software. If adversaries can get malicious code onto the computer, they can modify or disable the encryption, allowing the disk to store unsecured data. NSA recently removed several software encryption solutions from the DaR CSfC Component List due to discovered vulnerabilities that weaken key strength. Software encryption tools also share processing resources, which causes latency when encrypting, negatively affecting the user experience and productivity.

Self-encrypting drives (SEDs) have gained popularity due to their ability to perform encryption operations on a dedicated crypto processor that is part of the drive controller. This gives them several, mainly performance-related, benefits compared to software-based encryption products which rely on the computers processor (CPU). The main security benefit with SEDs is that the encryption key is an input at boot time which makes it less exposed to theft. However, SEDs too have known vulnerabilities. This is due to the ability to covertly access the drive when the host system is turned on, or in sleep mode[1].

The main risk with commercial encryption products is that they are available for unrestricted purchase to anyone willing to pay for them. Regardless of how good the technology is, or how strong the encryption, once a threat actor has access to a product's configuration, it becomes a matter of time until it can be compromised.

Enter Password

Please enter password or provide key file to encrypt selected files on your computer.

Origin: Delete original files after encryption.

Key file

Figure 1: Commercial DaR Encryption Options

CSfC Solutions (Medium Risk)

Established by NSA, CSfC allows programs to develop their own solutions to protect classified data in compliance with established Capability Packages. CSfC solutions involve layering multiple COTS products from an Approved Products list according to Capability Packages. Due to the use of COTS products, these solutions require yearly registration and continuous maintenance to ensure compliance, which can result in higher overall life cycle cost.

High Assurance Type 1) Encryption (Low Risk)

High assurance Type 1 DaR devices are hardware solutions that have been certified by NSA to protect data up to Top Secret/SCI and below. The NSA certification process is a rigorous development and testing process that eliminates the risk the organization or IA authority has to assume during the ATO process. These devices use the latest NSA approved algorithms and security architectures, and are employed according to NSA developed operational doctrine. Due to the sensitive nature of their design, high assurance Type 1 devices are only available to the U.S. government, and federally sponsored non-U.S. government activities (e.g. contractors or coalition/mission partners) subject to International Traffic in Arms Regulations (ITAR).

In addition to meeting DoD requirements for classified DaR protection, high assurance Type 1 devices offer multiple operational benefits discussed below.

HIGH ASSURANCE TYPE 1 DaR USE CASES

Tactical Vehicles/ISR Platforms

Tactical platforms operate in hostile and uncontrolled environments and require protection of their mission logs and/or collected surveillance data. Classified information stored onboard is required by law to have cryptographic protection in the event of compromise. In June of 2019, an American surveillance drone was shot by Iran in over the Strait of Hormuz. Without high assurance protection, data onboard this platform is at high risk of becoming intelligence for an adversary.

Incidents like this have led to requirements for defense programs to comply with enhanced cryptographic standards. This entails

[1] *Bypassing Self-Encrypting Drives (SED) in Enterprise Environments, Nov 2015, Boteanu, Fowler; KPMG*

Figure 2: U.S. ISR drone shot down by Iran in June 2019

designing new platforms, as well as retrofitting legacy platforms to accommodate secure data storage capabilities. Integrating new technology into an existing architecture poses challenges including size, weight and power (SWaP) concerns as well as security implications to the host system(s). Fortunately, newer off the shelf high assurance Type 1 DaR devices are designed for easy integration into legacy systems, enabling programs to enhance security and also avoid lengthy system certification delays.

Additionally, the increased use of unmanned ISR platforms has created the need to manage crypto remotely, autonomously detect when a threat incident is occurring, and take action to protect the data stored onboard. Today's autonomous military systems are in their infancy, and it is imperative that tomorrow's systems are developed with these safeguards in mind. General Dynamics Mission Systems offers the ProtecD@R® Multi-Platform Encryptor (KG-204), currently the only high assurance DaR encryptor that supports unattended operation.

Secure Data Transport

Transporting classified DaR can be an onerous, time consuming, and costly task. Consider a scenario where users gather classified data at a test event that must be sent to an alternate location for analysis at the speed of relevance. Without high assurance Type 1 encryption, storage media containing classified data must be handled at its designated classified level. This places restrictions on transporting, increasing the time (days/weeks) between data collection and analysis. When classified data is encrypted with a high assurance Type 1 device, the storage media can be handled as unclassified and shipped via commercial couriers (e.g. FedEx), greatly improving time to analysis and decision cycles.

A similar scenario exists with transporting drives between a platform's air and ground stations. When the aircraft lands, if protected with high assurance Type 1 encryption, the drives can be transported as unclassified to the ground station for analysis.

Forward deployed units can also ensure data collected in the field is protected if a security event occurs and storage media is compromised.

Enterprise Applications

Public and private sector data breaches have become routine headline news, and it is imperative defense organizations insulate themselves from this risk. Whether it is the theft of a PC from an unattended desk, or a drive from a data center storage array, the potential for the insider threat attack is real. The future of high assurance DaR encryption will assign specific keys to individual users allowing for tighter security and data tracking across the enterprise and cloud environments. This will restrict users from accessing unauthorized data unless they have the assigned key for that specific dataset. Future high assurance solutions will also protect data as it is stored in a cloud environment.

Defense organizations have been tasked with supporting the Federal Data Center Optimization Initiative (DCOI). In order to support multiple security levels (unclassified through Top Secret/SCI) individual storage arrays or even the datacenters themselves are separated, increasing the number of arrays, and ultimately datacenters. As illustrated in Figure 3, high assurance Type 1 encryption will support consolidation initiatives by allowing multiple classification levels to be stored within a single storage array and location, providing significant cost savings associated with facilities, overhead and equipment.

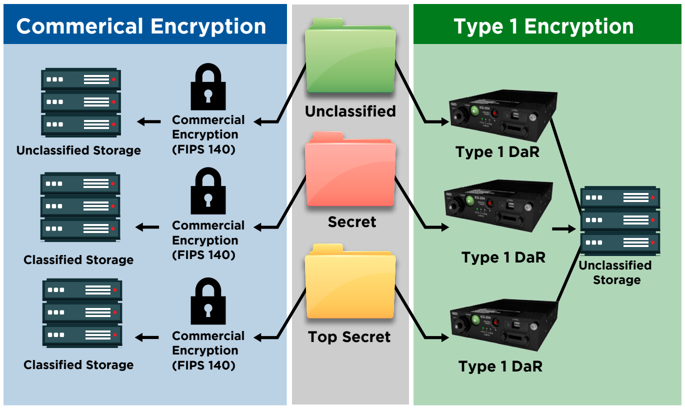

Figure 3: Storage consolidation with high assurance Type 1 DaR

Storage Media Reuse

When deleting files from a storage drive it is possible for residual data to remain on the underlying media, leaving information available to an adversary in the event a drive is lost or stolen. This must be a consideration for drives storing classified information. NSA has issued guidance for secure file deletion for both Hard Disk Drives (HDD, i.e. spinning disk drives), as well as Solid State Drives (SSD) in the NSA/CSS Storage Device Sanitization Manual (Dec 2017).

[2] *U.S. Code, Title 44, Chapter 35, Subchapter II, § 3557, National Security Systems*

Commercial SSDs storing classified information must be destroyed after use if not encrypted with high assurance Type 1.

However, since SSDs do not always present all memory as accessible, there are no guarantees these methods will result in complete data removal, and the recommendation is to destroy after use. DoD organizations can implement various policies and procedures to sanitize or purge drives before reuse, such as the Army's Pamphlet 25-2-3, "Reuse of Army Computer Hard Drives", however these are basic guidelines as specific sanitization is dependent on the type of media and manufacturer.

To avoid these arduous procedures, and the risk of partial data erase, many DoD organizations destroy storage drives after the crypto period of the classified data expires. Given that the recommended crypto period for most data is a maximum of one year, this can significantly impact hardware and logistics costs during a programs lifecycle.

THE BOTTOM LINE

The number of malicious actors in today's cyber environment is ever increasing, driving up the critical importance of protecting our Nation's most sensitive stored data. The decision to protect your DaR is ultimately a question of how much risk are you willing to accept? What could an adversary do if they got access to your sensitive data?

Contact us for more information:

E: infosec@gd-ms.com
W: GDMissionSystems.com/DaR
P: 888-897-3148 | 781-410-9400

TYPE 1 DaR SOLUTIONS

General Dynamics Mission Systems is making it easier for DoD programs to meet their DaR encryption requirements with the ProtecD@R® portfolio of DaR encryptors.

PROTECD@R
BECAUSE DATA AT REST IS DATA AT RISK

Built for use from the enterprise to the edge, ProtecD@R encryptors offer flexible designs to protect stored data on an array of platforms and devices. Our current portfolio includes:

ProtecD@R Multi-Platform (KG-204):

- The only DaR encryptor designed to support unattended operations and protect information classified up to TS/SCI and below.
- Supports data throughput speeds up to 24GB/s (SATA III), OS agnostic.
- Certified by NSA in 2020.

ProtecD@R High Speed (KG-540A/B):

- The fastest high-speed DaR encryptor available. For larger platforms and higher speed enterprise.
- 32Gb/s throughput (Infiniband), supports data up to TS/SCI and below, airborne and ground station variants available.

Custom Solutions:

General Dynamics Mission Systems has built custom DaR solutions around specific end customer and program needs. Contact us to discuss if these solutions can meet your requirements, or if we can tailor a solution to address your specific needs.