THE GOVERNMENT CONTRACTOR®

THOMSON REUTERS

Information and Analysis on Legal Aspects of Procurement

Vol. 62, No. 8 **February 26, 2020**

Focus

¶ 47

FEATURE COMMENT: Be Sure To Drink Your Ovaltine—The DOD Cybersecurity Decoder Pin For Federal Encryption Standards

Be sure to drink your ... Ovaltine. Ovaltine?
A crummy commercial!?
Ralphie Parker—*A Christmas Story*

In the seminal holiday film *A Christmas Story*, nine-year-old Ralphie Parker uses his diligently earned Little Orphan Annie Secret Society decoder pin to decrypt the secret message from Annie to her fans, only to express disappointment and confusion when he realizes the "secret code" he decrypted is nothing more than a marketing ploy to sell more Ovaltine. Although neither drinking copious amounts of Ovaltine nor possessing a Little Orphan Annie decoder pin are requirements of a federal contractor's cybersecurity program, the use of encryption—like that employed by Ovaltine and its plucky propagandist—cannot be avoided. The challenge, of course, is approaching encryption in a manner that avoids the same irritating bewilderment experienced by Ralphie Parker. Modern encryption, while inherently and necessarily enigmatic, need not be overcomplicated, and that's a good thing, because federal contractors, namely Department of Defense contractors, now face specific standards of encryption necessary to meet and maintain certain federal cybersecurity standards or bear the significant risk commensurate with noncompliance. Whether a contractor falls under the auspices of Federal Acquisition Regulation 52.204-21, Defense FAR Supplement 252.204-7012, or the newly unveiled Cybersecurity Maturity Model Certification (CMMC), contractor use of encryption is poised to be a critical element of compliance for the Federal Government over the next decade. This means that contractors must have a working knowledge of federal encryption standards to understand not only how such standards apply to the storage and handling of data but also whether the contractor can truly comply with those standards or have the wherewithal to understand the type of information technology products they are permitted to provide the Government.

Encryption—In its most basic form, encryption is the algorithmic process of converting data from its original form (plaintext) into an encoded text (ciphertext). To access the encrypted data, an individual must use the required cryptographic key to decrypt the data. This permits data—be it sensitive or mundane—to become completely incomprehensible to anyone not in possession of the cryptographic key, thereby enhancing data confidentiality, data integrity authentication and source/identity authentication. For example, when implemented correctly, the Advanced Encryption Standards (AES) type of encryption—the specification for the encryption of electronic data established by the Department of Commerce's National Institute of Standards and Technology (NIST)—is able to encrypt data using an algorithm that is nigh impossible to break, barring access to a state-of-the-art supercomputer and *885 quadrillion years* of time necessary to "crack" an AES-128 key by force. Ultimately, in addressing encryption and cryptography generally, it is the security of the key, not the security of the encryption algorithm—many of which are publicly available—that defines security.

But the *type* of encryption is only one piece of the puzzle; the *methods* used to transmit and decrypt encrypted data can impact the ultimate security of the data in transit. For example, the "end-to-end encryption" model, dubbed the "gold standard" method of encryption, encrypts data directly on the sender's device, keeps the data encrypted through transmission, and permits the data to be decrypted only once it reaches the recipient's

device. When done properly, end-to-end encryption ensures that third parties—such as internet service providers (ISPs), server hosting services, cloud providers transmitting and storing the encrypted data, and the ne'er-do-wells who attempt to exploit those services—never can (1) access the data or (2) access the means of decryption. Thus, this method permits the data to remain encrypted, and therefore protected, throughout all stages of transmission and storage, even if an ISP, server hosting service or cloud provider is compromised.

As a result of the widespread use of encryption in both public and private arenas, NIST estimates that the use of encryption standards, such as its AES, has provided a global economic benefit of $250 billion over the past 20 years. Further, DOD has voiced strong support for using cryptography to protect not only the nation's military and intelligence capabilities but also its economic security. With worldwide economic losses from cybercrime estimated as totaling $600 billion in 2017 and reaching $2 trillion in 2019 and the escalating incidents of brazen cyber espionage perpetrated by foreign actors and nation states, it is obvious why the security and reliability of encryption are important components of the Government's evolving cybersecurity requirements.

The following is intended to provide federal contractors with a high-level overview—a decoder ring, if you will—of the primary encryption standards applicable to federal contractors (FIPS 197 and 140-2) and reveal how encryption standards function as key components of international and national data privacy standards as well as federal cybersecurity compliance programs (i.e., NIST SP 800-171, CMMC) and agency-specific programs (i.e., the Department of State, Directorate of Defense Trade Controls' recent interim final rule proposing an exemption for encrypted technical data and software controlled by the International Traffic in Arms Regulation (ITAR)).

Federal Encryption Standards: FIPS 197 and 140-2—The Federal Information Processing Standards (FIPS) are standards for use in nonmilitary Government computer systems, specifically when there are no acceptable industry standards or solutions for a particular Government requirement. Developed by NIST and approved by the secretary of commerce in accordance with the Information Technology Management Reform Act of 1996 and the Federal Information Security Management Act of 2002, FIPS publications include standards for, inter alia, encryption algorithms, encryption key storage and the storage of certain types of federal agency data.

FIPS publications can mandate a number of security procedures for securing sensitive but nonconfidential data. For example, FIPS 140-2, Security Requirements for Cryptographic Modules—specifically addressed in the assistant secretary of the Navy's Sept. 28, 2018, memorandum "Implementation of Enhanced Security Controls on Select Defense Industrial Base Partner Networks"—requires contractors to implement physical security safeguards that conform with four different levels of security. Other FIPS standards, such as FIPS 197, Advanced Encryption Standard, provide standards on the algorithm used to actually encrypt the sensitive information. Both FIPS 197 and 140-2, as well as the in-development FIPS 140-3 (the upcoming successor to FIPS 140-2), are summarized below.

FIPS 197: Issued on Nov. 26, 2001, FIPS 197 "specifies a FIPS-approved cryptographic algorithm," the AES, "that may be used by Federal departments and agencies when an agency determines that sensitive (unclassified) information ... requires cryptographic protection." Concerned with the security implications resulting from recent advances in computing power at the end of the twentieth century, NIST selected the AES, a symmetric-key encryption method based on the Rijndael cipher, to replace the prior Data Encryption Standard in use since 1976. Notwithstanding the development of other FIPS-approved block ciphers over the years, AES remains the primary encryption standard for the Federal Government.

Although a primer on the inner workings of the AES algorithm is *far* beyond the scope of this article, it is, at its most rudimentary, a symmetric block cipher (i.e., the same key is used for encrypting and decrypting data) that can process 128-bit data blocks using cipher key lengths of 128, 192 or 256 bits. The practical takeaway is simple: the longer the cipher key, the more robust the encryption.

Under FIPS 197, NIST also validates a contractor's encryption engine to ensure that it meets FIPS-approved cryptographic standards (i.e., AES) through its Cryptographic Algorithm Validation Program (CAVP). The CAVP process employs accredited, third-party labs to validate a contractor's use of the AES in the contractor's encryption module, program or application. Once that encryption is validated, the contractor's algorithm details, operational environment, and

validation date are added to NIST's validation list for use by the Government and/or contractors.

However, CAVP validation is only one step in the process to meet the Government's standard for protecting sensitive but unclassified information—the contractor's module or application also must be validated as meeting the FIPS 140-2 criteria explained below. Put another way, FIPS 197 validation generally serves as only the contractor's *first step* in meeting federal encryption standards that may be resident in federal contracts.

FIPS 140-2: Aptly titled "Security Requirements for Cryptographic Modules" and administered by NIST, the FIPS 140-2 standard provides the mandatory requirements for, inter alia, the physical security of cryptographic modules—i.e., "the set of hardware, software and/or firmware that implements approved security functions (including cryptographic algorithms [such as AES], key generation, digital signatures, and authentication) and is contained within the cryptographic boundary"—protecting sensitive but unclassified information.

FIPS 140-2-validated cryptographic modules are required by federal agencies (and the contractors working with federal agencies) that "use cryptographic-based security systems to protect sensitive information in computer and telecommunications systems." With so much riding on the enforcement of the FIPS 140-2 standards, the importance of a federal contractor's adherence to these measures when selecting a cryptographic module or similar hardware for use in an IT system cannot be overstated. Nonetheless, contractors should take note that although the FIPS 140-2 security requirements are geared toward ensur-

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

ing the security of cryptographic modules, adherence to these FIPS requirements is but one of many elements in a responsible contractor's cybersecurity plan. The contractor is ultimately responsible for ensuring that (1) the security provided by a particular module "is sufficient and acceptable to the owner of the information that is being protected, and that any residual risk is acknowledged and accepted[,]" and (2) the contractor's "overall" system security is "appropriate for the security requirements of the application and environment in which the module is to be utilized and for the security services that the module is to provide."

As summarized in the chart below, the FIPS 140-2 standard specifies four security levels for each of eleven requirement areas.

In its design of FIPS 140-2, NIST recognized that not all data are the same, and the FIPS standard allows for cost-effective solutions that take into account the different degrees of data sensitivity and application environments, a concept not dissimilar to the model employed by DOD for data security under the CMMC. Therefore, each "level" of FIPS 140-2 offers an increase in protection over the previous level:

- *Level 1:* Provides the lowest level of security and specifies the minimal requirements for a cryptographic module—basically, that the module use at least one approved algorithm (e.g., AES) or security function. Appropriate for low-level security applications when other controls (e.g., physical security, network security) are absent.
- *Level 2:* Adds requirements for, among other measures, physical security mechanisms to a Level 1 cryptographic module by requiring the use of tamper-evident coatings or seals on the module to alert users when an attempt is made to access the plaintext cryptographic keys and critical security parameters within the module.
- *Level 3:* Requires, among other security enhancements, the use of identity-based authentication mechanisms to verify the identity of a user and to determine whether the specific user is authorized to use the cryptographic module for a specific task.
- *Level 4:* Provides the highest level of protection required under the FIPS 140-2 regime and is recommended only for situations where the cryptographic module will likely be subject to repeated access attempts by unauthorized users. Any unauthorized attempt to access the module will result in the immediate "wiping" of all critical security parameters (i.e., cryptographic keys, authorized passwords, and personal identification numbers).

Most contractors aim to meet Level 1 and 2 validation; validation at Levels 3 and 4 is relatively rare, as meeting such standards demands expensive hardware features for use in only the most unprotected environments.

Validation of cryptographic modules in accordance with FIPS 140-2 is performed by the Cryptographic Module Verification Program (CMVP), a joint operation of NIST and the Computer Security Establishment of Canada. CMVP validation, typically a long and costly process, is performed by accredited, third-party labs to "promote the use of validated cryptographic modules and provide Federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules." Once these cryptographic modules are successfully validated under the CMVP, they will be considered conforming to the FIPS 140-2 standard and thus permissible for use by the Federal Government or use by contractors for Government data.

Contractors should note the substantial difference between having a FIPS 140-2-*validated module* or product and a FIPS 140-2-*compliant module* or product. A validated module attests that a contractor's module or product has been subjected to the entire FIPS 140-2 validation process, resulting in certification by NIST. By contrast, a compliant module is a self-designated term without a NIST-approved analog. Contractors may use this compliant designation in reference to a module or product that uses a FIPS-197-compliant algorithm but has not actually been subjected to the CMVP testing process. Obviously, this means that there is a significant advantage to a contractor having a FIPS 140-2-validated product for sale to the Government and/or its contractors when mulling over whether the outlay of time and money for CMVP validation will be justified.

FIPS 140-3: In March 2019, NIST announced the development of FIPS 140-3, the iterative version of the 18-year-old FIPS 140-2 standard. This updated version incorporates the Government's decision to adopt, with some modifications, previously existing international cryptographic standards International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19790:2012 (the security requirements for a cryptographic module utilized within a security system protecting sensi-

tive information in computer and telecommunication systems) and ISO/IEC 24759:2017 (the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012). Although FIPS 140-3 was officially released on Sept. 22, 2019, testing on this standard is not expected to begin until September 2020 at the earliest, and FIPS 140-2 testing and validation will continue for a year after FIPS 140-3 validation goes into effect. Thus, both agencies and contractors will have time to meet this new standard once it finally is vetted.

Encryption Standards in Practice—With a basic understanding of the cryptographic process in hand, this section will highlight how encryption standards are integrated into data privacy and federal cybersecurity compliance programs and are also being used in agency-specific programs.

Encryption and Personal Privacy Regulations: The modern data privacy revolution effectively began in earnest on May 25, 2018, when the European Union's (EU) General Data Protection Regulation (GDPR) took effect, attempting to protect a wide array of personal data pertaining to EU data subjects with a regime intended to be enforceable against parties anywhere in the world. See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. The GDPR gives EU residents certain rights and requires that legal entities, whether companies or persons, that process personally identifiable data take certain precautions to protect it. Among other tasks, these entities must have a legal basis to process the personal data, implement "appropriate" technical and organizational measures to protect the personal data, and alert residents in the event of a data breach that is likely to result in a high risk to the rights and freedoms of EU data subjects. While the GDPR is not clear on what exactly are appropriate technical measures, it does indicate that encryption can be appropriate. The GDPR provides further that in the event of a personal data breach, the data holders, or controllers, are required to notify the affected EU residents to whom the breached data pertains if the breach is likely to result in a high risk to those individuals' personal rights and freedoms. Notably, however, if the controller applied appropriate technical and organizational measures to that data, such as encryption, it would not need to notify the affected parties. While such a tool may not relieve the controller from having to report the breach to governmental or quasi-governmental agencies, it would limit the impact and cost associated with the breach by eliminating the need to notify each individual or to protect its global reputation.

A little closer to home, the privacy revolution landed most loudly on the west coast with the passage of the California Consumer Privacy Act (CCPA). See California Civil Code § 1798.100 et seq. While the CCPA does differ from the GDPR in some regards, it shares an affinity for implementing reasonable security measures and practices appropriate to the nature of the personal information. Like the GDPR, the CCPA permits a private right of action in the event of a data breach where personal data is "nonencrypted and nonredacted" at the time of the breach. This language is key because it allows businesses (the CCPA equivalent of the GDPR's "controllers") to sidestep the risk of the private right of action (unlike the GDPR), because in order to obtain civil damages (up to the greater of $750 or actual damages per person subject to the breach), the plaintiff would have to show that the business neither encrypted nor redacted their information. Whether for a purely commercial vendor or a federal contractor, in the realm of data privacy, encryption is becoming a very common, cost-efficient and easily implemented measure to avoid significant risk.

NIST SP 800-171: NIST Special Publication (SP) 800-171, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, provides federal agencies with recommended security requirements for protecting the *confidentiality* of Controlled Unclassified Information (CUI) when (1) the CUI is resident in a nonfederal system and organization, (2) the nonfederal organization is *not* collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency, and (3) there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or Government-wide policy for the CUI category or subcategory listed in the CUI Registry. A NIST SP is similar to a FIPS, but a SP neither requires the prior approval of the secretary of commerce nor is mandatory unless a particular Government agency (e.g., DOD) makes it so.

Specifically, NIST SP 800-171 recommends security requirements applicable only to "components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such com-

3.1 Access Control	3.1.13 – Employ cryptographic mechanism to protect the confidentiality of remote access sessions. 3.1.17 – Protect wireless access using authentication and encryption. 3.1.19 – Encrypt CUI on mobile devices and mobile computing platforms.
3.5 Identification and Authorization	3.5.10 – Store and transmit only cryptographically protected passwords.
3.8 Media Protection	3.8.6 – Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
3.13 System and Communications Protection	3.13.8 – Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. 3.13.10 – Establish and manage cryptographic keys for cryptography employed in organizational systems. 3.13.11 – Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

ponents" and are intended for use by federal agencies "in appropriate contractual vehicles or other agreements established between those agencies and nonfederal organizations." As of Dec. 31, 2017, contractors that store or control Covered Defense Information (CDI), which includes CUI, must be compliant with the NIST SP 800-171 requirements as mandated by certain federal regulations, most notably pursuant to DFARS clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*.

The NIST SP 800-171 framework specifies 14 "families" of security requirements for CUI, such as "Access Control," "Configuration Management," "Incident Response," "Physical Protection," and "System and Information Integrity." Each family listed above includes a subset of specific requirements divided between "basic security requirements" and "derived security requirements." Notably, a number of NIST SP 800-171 security requirements specify the use of cryptographic mechanisms for compliance.

The NIST SP 800-171 requirements for cryptography used to protect CUI—typically when CUI is transmitted or stored *outside* the contractor's IT system (including wireless and/or remote access) and not separately protected—must use "FIPS-validated cryptography," which means that the cryptographic module has *been tested and validated* through the CMVP (and, as a prerequisite, the FIPS 197-assessing CAVP) to meet FIPS 140-2 requirements. As noted previously, solely using an approved algorithm, such as AES, to encrypt data is not sufficient to meet the FIPS 140 standard. Rather, to comply with the FIPS 140 standard, the cryptographic *module* employing the algorithm must be *separately* validated under the FIPS 140-2 rubric. Notably, encryption used in situations when the CUI remains *inside* the protected environment of the contractor's information system would *not* need to be FIPS-validated.

CMMC—As many readers of this article are aware, the office of the undersecretary of defense for acquisition and sustainment, with input from DOD stakeholders and other entities, has been actively developing the CMMC framework with the goal of enhancing the protection of Federal Contract Information (FCI) and CUI for the entire Defense Industrial Base supply chain. Covering vendors from builders of major weapon systems to providers of custodial services, the CMMC framework is expected to apply across DOD to a variety of effects. Although CMMC Version 1.0 was released only in late January 2020, contractor compliance with the CMMC will be a mandate prior to doing business with DOD entities.

The CMMC combines various cybersecurity control standards, such as NIST SP 800-171 and NIST SP 800-53, into one unified standard for cybersecurity. At its simplest form, the CMMC encompasses a set of 17 "domains" mapped across five increasing levels (Levels 1 to 5) of cybersecurity. Each domain is made up of certain "capabilities" (43 in total) to ensure security within each domain; each capability is further broken down into 171 "processes and practices" (i.e., the "processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references"). As the CMMC draws heavily from, among other sources, NIST SP 800-171, it's no surprise

that contractor compliance with the CMMC at certain levels *also* requires compliance with NIST SP 800-171 encryption standards. From subsets of SP 800-171 requirements found at Levels 1 and 2 to the full complement of SP 800-171 requirements at Level 3, defense contractors will need to be familiar with and generally compliant with, among other standards, many or *all of the* NIST SP 800-171 security requirements. Notably, as it relates to CMMC 1.0, encryption requirements are found within the following processes.

As noted above, the application of encryption riddles the CMMC—and it's not focused on just Level 3. For Levels 2 and up, no compliant DOD contractor will be able to evade the need to properly encrypt the FCI and/or CUI resident in or generated by their respective contracts.

The DDTC's "End to End Encryption" Interim Final Rule—On Dec. 26, 2019, the State Department's Directorate of Defense Trade Controls (DDTC) issued its belated interim final rule clarifying that specific transfers of encrypted technical data are not exports, reexports, or retransfers subject to the ITAR. This interim final rule harmonizes the ITAR and Export Administration Regulations (EAR) regarding the use, transfer and storage of properly encrypted technical data. In sum, the harmonization provides that transfers of ITAR-controlled data meeting the interim final rule's encryption requirements will not be deemed "exported" under the ITAR regulations and thus will not require DDTC authorization to be moved. Specifically, "the properly secured (by end-to-end encryption) electronic transmission or storage of unclassified technical data via foreign communications infrastructure does not constitute an export, reexport, retransfer, or temporary import."

To us, the key takeaway from the DDTC's interim rule is the importance of the application/use of end-to-end encryption when storing, sending and transporting unclassified information. This means that the data being transmitted must (1) be properly encrypted (e.g., using a compliant FIPS 140-2 cryptographic module and supplemented by applicable NIST standards and controls, *or* by other cryptographic means at least comparable to the AES-128 security strength) when it leaves the sender's in-country security boundary; (2) remain encrypted until decrypted by the intended authorized recipient within the recipient's in-country security boundary; or, (3) in the case of remote storage, be retrieved by the sender. That is, for the DDTC's exception to apply, the cryptographic protection applied to the data must not be removed at any point during the transmission and storage process until decrypted by the authorized, intended recipient or owner. To ensure this level of security and to meet the DDTC's definition of end-to-end encryption, it is critical that the means of decrypting the data, meaning the key, must not have been provided to or stored by *any* third party, such as an ISP, server hosting service, or cloud provider. Notably, the DDTC declined to expand its interim final rule to exempt from DDTC authorization controlled technical information secured with either "tokenization" (a process that replaces elements of a document with representative "tokens" rather than us-

CMMC Level	Process	Description
3	AC.3.012	Protect wireless access using authentication and encryption.
3	AC.3.014	Employ cryptographic mechanisms to protect the confidentiality of remote-access sessions.
3	AC.3.022	Encrypt CUI on mobile devices and mobile computing platforms.
5	CM.5.074	Verify the integrity and correctness of security critical or essential software as defined by the organization (e.g., roots of trust, formal verification, or cryptographic signatures).
2	IA.2.081	Store and transmit only cryptographically protected passwords.
3	MP.3.125	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.
2	SC.2.179	Use encrypted sessions for the management of network devices.
3	SC.3.177	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.
3	SC.3.185	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.
3	SC.3.187	Establish and manage cryptographic keys for cryptography employed in organizational systems.

ing an algorithm to encrypt) or encryption, stating "[t]here is no NIST or other comparable standard that the Department can reference to set a minimum threshold for implementation of tokenization."

The practical result of the DDTC's interim final rule, when considered in tandem with the EAR's similar existing provisions regarding the transmission and storage of controlled technologies and technical data, is that contractors will have yet another incentive to encrypt data to the benefit of national security and their own internal efficiencies.

So Why Does Encryption Matter?—As described above, encryption provides contractors with one of the most (if not *the* most) secure forms of data transmission. When operating in the current landscape of global commerce, data security is paramount. Using a narrower lens, encryption is a key component of the major federal cybersecurity programs to which all federal subcontractors must adhere and, in the case of data privacy, it provides a cost-effective means to mitigate and even eliminate litigation risk. To meet (and maintain) these significant standards, contractors must have a working knowledge of the mandated levels of encryption when transmitting or storing sensitive federal information. Fortunately, modern encryption products are far less clunky than the encryption programs of the past. Federal contractors need not feel as though encryption will bog down their systems as if swaddled in an overstuffed coat or tie them to networks as if their tongues were stuck to a frozen flagpole. Rather, the increasing demand and need for such products are creating platforms and solutions that are becoming increasingly easier to use and deploy. With the penalties for contractors with noncompliant IT systems increasing exponentially, it's worth a lifetime's supply of Ovaltine for contractors to get serious about federal encryption standards, find the tools necessary to meet their contractual obligations, and, of course, not shoot their eye out.

✦

This Feature Comment was written for THE GOVERNMENT CONTRACTOR by* Alex Major, Ethan Brown *and* Morgan Jones*, attorneys at McCarter & English LLP.