ROGERS | JOSEPH | O'DONNELL

Not What it Seems:
The June 2023 DHS Final Rule on Safeguarding Controlled Unclassified Information

By Robert Metzger, Deborah Rodin, Cindy Lopez, and Julia Caruso
Mr. Metzger is a Shareholder; Ms. Rodin, Ms. Lopez and Ms. Caruso are Associates of the Firm

I. INTRODUCTION

On June 21, 2023, the Department of Homeland Security (DHS) issued a final rule, "Safeguarding of Controlled Unclassified Information" (CUI). 88 Fed. Reg. 40560 (June 21, 2023). The rule amends the Homeland Security Acquisition Regulation (HSAR) and adds three new contract clauses, 48 CFR 3052.204–71, 3052.204–72, and 3052.204–73, to address requirements for the safeguarding of CUI.

The stated impetus behind the rule is the "*urgent need to protect CUI* and respond appropriately when DHS contractors experience incidents with DHS information." 88 Fed. Reg. at 40560 (emphasis added). Citing "pervasive high-profile breaches of Federal information," the rule points to "the need to ensure that information security protections are clearly, effectively, and consistently addressed in contracts." *Id.* The new HSAR clauses feature security and privacy measures to protect CUI, as well as requirements to facilitate improved incident reporting to DHS. The final rule becomes effective July 21, 2023.

II. BRIEF SUMMARY

More than six years since DHS published its ***proposed*** rule on safeguarding CUI, the final rule features a broad framework of requirements and procedures to ensure the protection of CUI in DHS procurements. It is not, in the authors' analysis, broadly applicable to the thousands of ordinary companies who furnish supplies and services to DHS and its many components. To the contrary, it applies to a much smaller, and more select, group: those contractors who operate a Federal information system "on behalf of" DHS.

- This rule says little about how "ordinary" DHS contractors are to protect CUI. In fact, it largely avoids this obviously important subject and instead repeatedly references a possible "FAR CUI" rule as the eventual source of requirements relevant to most DHS contractors.

- The DHS rule does not rely on NIST SP 800-171 as the baseline for applicable cybersecurity standards, as DoD employs for its CUI protection rules already applicable to tens of thousands of companies in the Defense Industrial Base (DIB).

- Instead, because the DHS rule explicitly is to address the safeguarding requirements specified in the Federal Information Systems Modernization Act of 2014 (FISMA), which apply to federal entities and not to commercial (nonfederal) organizations, it uses the cyber standards of NIST SP 800-53.

- Again, distinct from DoD, the DHS rule uses a different definition of CUI to be protected, emphasizes protection of CUI categories created by DHS that are distinct from those that are the focus of DoD, and it seeks protection not only of "confidentiality" but also, as FISMA requires, of "integrity and availability."

- Further the DHS Rule contemplates third-party assessment only for the limited set of companies who seek authorization to operate information systems for or on behalf of DHS and its components; in contrast, it is DoD's intention, in its CMMC initiative, to require independent assessment of thousands of DIB suppliers.

- Lastly, and for similar underlying reasons, the incident reporting obligations of this rule are both broader in scope and use shorter deadlines than the DoD CUI rules.

The DHS final rule becomes effective on July 21, 2023. Contractors for DHS should review the new rule carefully, first to determine if it applies to them, and, if so, to plan for how they will satisfy its requirements. This analysis may help inform companies whether they are subject to the new DHS Rule.

III. BACKGROUND TO THE RULE

More than six years ago, in January 2017, DHS published a notice of proposed rulemaking that addressed the need to ensure the protection of CUI ("proposed rule"). 82 Fed. Reg. 6429 (Jan. 19, 2017). The 2017 proposed rule sought to implement adequate security and privacy measures to safeguard CUI and facilitate improved incident reporting to DHS by adding a contract clause that would:

> (1) Strengthen and expand existing HSAR language to ensure adequate security for CUI that is accessed by contractors; collected or maintained by contractors *on behalf of an agency*; and/ or for Federal information systems that collect, process, store or transmit such information;
>
> (2) Identify CUI handling requirements and incident reporting requirements, including timelines and required data elements;
>
> (3) Include inspection provisions and post-incident activities and require certification of sanitization of Government and Government-Activity related files and information; and
>
> (4) Require that contractors have in place procedures and the capability to notify and provide credit monitoring services to any individual whose Personally Identifiable Information (PII) or Sensitive PII (SPII) was under the control of the contractor or resided in the information system at the time of the incident.

82 Fed. Reg. 6429 (Jan. 19, 2017) (emphasis added).

Public comments on the proposed rule were due by March 20, 2017, and fourteen respondents submitted comments. DHS reviewed and discussed those comments in its newly published, final rule. The final rule departs from the 2017 proposed rule in four significant ways:

> (1) Identifies CUI handling requirements and security processes and procedures applicable to Federal information systems, which include contractor information systems operated *on behalf of DHS* (rather than on behalf of "an agency" as the proposed rule had stated);
>
> (2) Identifies incident reporting requirements, including more detailed timelines and required data elements, inspection provisions, and post-incident activities;
>
> (3) Moves the requirement for a contractor to have an Authority to Operate (ATO) before collecting, processing, storing, or transmitting CUI within a Federal information system to Alternate I from the basic clause; and
>
> (4) Moves requirements for PII, and SPII notification and credit monitoring requirements to a separate contract clause (HSAR 3052.204–73).

IV. APPLICABILITY

The DHS final rule applies to Federal information systems used to collect, process, store, or transmit CUI, including "contractor information systems operated *on behalf of*" DHS. To be clear, this means that ***the rule applies to contractor information systems that contractors operate directly for ("on behalf of") DHS***. The rule "recognizes that there are circumstances when contractor information systems are operated on behalf of an agency," and **"[w]hen this is the case, the contractor information system is considered a Federal information system and is subject to the same information system security requirements required for Federal information systems**." 89 Fed. Reg. at 40564 (emphasis added). The emphasized language has great importance. Commercial organizations who perform contracts with DHS to deliver supplies and services ordinarily do ***not*** operate an information system on behalf of DHS and they are ***not*** subject to the many obligations that attach to running a Federal information system.

Accordingly, this rule has limited effect on nonfederal systems which contractors are not being operated on behalf of the agency. So, the number of companies subject to this rule may prove to be much smaller than might be expected on first impression.

Indeed, in this final rule, DHS says little about what it expects its "ordinary" commercial suppliers to satisfy to protect CUI. In this regard, DHS has deferred, largely, to what it anticipates will be a new "FAR CUI rule that addresses the requirements nonfederal information systems must meet before processing, storing, or transmitting CUI." 88 Fed.

Reg. at 40565.[1] However, to the extent that recurring access to government facilities or CUI is required under a contract, the clause at HSAR 3052.204–72 would apply, using Alternate II, but not the ATO requirement under HSAR 3052.204–72 Alternate I.

Of note, these clauses do not take into consideration a contractor's business size.

V. KEY REQUIREMENTS

A. Policy

DHS requires CUI to be safeguarded when CUI resides on:

- DHS-owned and operated information systems,
- DHS-owned and contractor-operated information systems,
- contractor-owned and/or operated information systems ***operating on behalf of DHS***, and
- "any situation where contractor and/or subcontractor employees may have access to CUI because of their relationship with DHS."[2]

DHS also requires contractor employees who require recurring access to government facilities or access to CUI to fill out certain forms for security purposes, including individual employee background investigations.

B. Contract Clauses – Requirements & Applicability

The final rule amends the HSAR to provide three new mandatory contract clauses to be inserted in solicitations and contracts, applicable subcontracts, and in certain, specific situations, including in instances where employees of the contractor and subcontractor require ***recurring access to government facilities or access to CUI***. Contracts with educational institutions are exempt, however.

---

[1] Discussed further, *infra* n.3.

[2] HSAR 3004.470–3(a), 88 Fed. Reg. at 40598. The first three of these four items are relatively straightforward. The fourth ("any situation") is not. The language suffers several ambiguities. Is the "situation" one that results from contract performance or some other form of access? What may be types of a "relationship" that satisfies the causal ("because of") requirement? It is also unclear what safeguarding duties may apply under the fourth trigger. One may suspect this is a reference to the situation under Alternate II of HSAR 3052.204–71, where a contractor may have access to CUI or government facilities but does not operate on behalf of DHS or have access to information systems. If that is the case, then the restrictions in the Alternate II clause would apply. To date, DHS has not clarified or issued any further guidance in its policies and procedures available online.

For the purposes of the information systems subject to this rulemaking, a Security Requirements Traceability Matrix (SRTM) will be included in all applicable solicitations, using the controls from NIST SP 800–53. The type(s) of CUI provided and/or developed under the contract also will be identified in the solicitation. Where ***nonfederal*** information systems are used, DHS defers to the yet-to-be finalized FAR CUI rule but anticipates that NIST SP 800-171 will serve as the baseline for security controls; otherwise, DHS does not anticipate a change to the process of providing an SRTM and identifying the type(s) of CUI provided or developed under a contract.[3]

48 CFR 3052.204–71, Contractor Employee Access

The clause at HSAR 3052.204–71 must be included in solicitations and contracts when contractor and/or subcontractor employees require recurring access to government facilities or to CUI. This clause implements the requirement that contractor employees must complete certain forms necessary for security purposes, such as background investigations, and limits contractor employee access to CUI "only for the purpose of furnishing advice or assistance directly to the Government in support of the Government's activities." It also requires employee training on the protection and disclosure of CUI, with initial training to be completed within 60 days of a contract award, as well as subsequent "refresher training" every 2 years.

3052.204–71 Alternate I. For acquisitions requiring contractor access to government information resources, contracting officers must add the Alternate I clause, which mandates that contractor employees receive a security briefing in advance of gaining access to information resources and may require additional training for specified categories of CUI. There are additional restrictions on contractor access to DHS information resources and a prohibition on non-US citizens accessing or assisting in the

[3] The final rule makes nine references to "the FAR CUI Rule." DHS explains that the National Archives and Records Administration (NARA) is "working with the FAR Councils, in which DHS is a participant, to develop a FAR CUI rule that addresses the requirements that ***nonfederal information systems must meet*** before processing, storing, or transmitting CUI." 88 Fed. Reg. at 40565 (emphasis added.) DHS repeatedly admits that it is "intentionally silent" on the requirements applicable to nonfederal information systems, as the FAR CUI rule is intended to address the requirements applicable to those systems. *Id.* at 40564-40565, 40568. Contractors might construe the discussion of the FAR CUI rules to imply that its publication is imminent. The current OMB/OIRA Regulatory Agenda, at View Rule (reginfo.gov), refers to FAR Case 2017-016, by which DoD, GSA, and NASA, are proposing to amend the FAR to protect CUI. The latest report (Spring 2023) for this rulemaking action (RIN 9000-AN56) indicates that a proposed rule is due July 2023 and that the comment period for the proposed rule will end in September 2023. This rulemaking, however, has been in gestation since 2017, so further delays cannot be ruled out.

"development, operation, management, or maintenance of Department IT systems under the contract," absent a waiver.[4]

48 CFR 3052.204–72, Safeguarding of Controlled Unclassified Information

The "Safeguarding" clause at 48 CFR 3052.204-72 aims to ensure adequate protection of CUI from unauthorized access and disclosure. This clause is to be used as prescribed in HSAR 3004.470-4(b), which indicates that the Safeguarding clause must be included in two circumstances. First, the clause is required in solicitations and contracts where contractor and/or subcontractor employees will "have access to CUI," or "where CUI will be collected or maintained on behalf of the agency." HSAR 3004.470-4(b)(1). Second, the basic clause *with its alternate* is to be included "when Federal information systems, which include contractor information systems operated *on behalf of the agency*, are used to collect, process, store, or transmit CUI." HSAR 3004.470-4(b)(2) (emphasis added).[5]

The Safeguarding clause, at HSAR 3052.204-72(b), states that contractors and subcontractors "must provide adequate security" to protect CUI from unauthorized disclosure. Previously, at 3052.204-72(a), "adequate security" was defined as:

> security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

[4] Clause 3052.204–71 also has an Alternate II that remains unchanged from the prior version of the rule and is relevant where contractors' and subcontractors' employees will not have access to government information resources but where DHS has determined that employee access to CUI, sensitive information, or recurring access government facilities must be limited to U.S. citizens and lawful permanent residents. This is a remnant of the prior clause (June 2006) that now poses an ambiguity. In the new rule, DHS has limited the applicability of these clauses to DHS contractors and systems operated on behalf of DHS, but here, obligations may exist where recurring access to "government facilities" occurs.

[5] While the DHS rule emphasizes that it is not intended to apply to commercial information systems, excepting those used on behalf of the agency, the language of HSAR 3004.470-4(b)(1) might be interpreted more broadly. If a contractor supplies goods or services to DHS, and is provided CUI by DHS for its performance, DHS might maintain that the hosting (or storage) of that CUI means that it is "maintained [by the contractor] on behalf of the agency." To avoid unexpected (and likely unintended) application to ordinary contractors, DHS should clarify its intentions.

88 Fed. Reg. at 40600.[6] However, at HSAR 3052.204-72(b)(1), which restates the obligation to protect CUI from unauthorized disclosure and access, the definition of "adequate security" is supplemented:

> Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors.

88 Fed. Reg. at 40601. This definition of "adequate security" differs from the one relied on by the Department of Defense for its rule on safeguarding CUI, as is discussed further in the Assessment section.[7] The reference to separate policies and procedures means that the obligations of contractors, where subject to this rule, are not set by a baseline NIST standard, but may change as the policies and procedures evolve. This section also contains restrictions on contractor handling of CUI, including that contractors cannot maintain SPII in their invoicing, billing, or other recordkeeping systems, for instance.

In 3052.204-72(c) and (d), the clause identifies incident reporting requirements, including timelines and required data elements, inspection provisions, and post-incident activities. It states that "all known or suspected incidents" must be reported to DHS' Component Security Operations Center (SOC) within 8 hours of discovery, and all incidents involving PII or SPII must be reported within 1 hour of discovery.[8]

Finally, the clause at 3052.204-72(e) requires that, upon conclusion of the contract, the contractor must return all CUI to DHS and/or destroy it in accordance with the NIST guidelines for sanitization of government and government-activity related files and

---

[6] This definition encompasses protection of "confidentiality, integrity, and availability," which is consistent with FISMA requirements to security of Federal information systems. In contrast, DoD's security requirements for commercial (nonfederal) organizations, as expressed in DFARS 252.204-7012 and NIST SP 800-171, focus on "confidentiality" objectives.

[7] It also differs from the NIST definition of "adequate security," which is "[s]ecurity commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." The combined definitions of "adequate security" may prove frustrating to both DHS and its contractors – even those who operate information systems on behalf of the agency. This definition is analogous to a "performance specification." Excepting systems subject to an Authorization to Operate under its Alternate I, HSAR 3052.204-72 does not invoke an established process or framework, such as the NIST Risk Management Framework (RMF), and does not articulate which of the potentially relevant controls in NIST SP 800-53 should apply.

[8] While prompt notification of security incidents is obviously important, it is also important to have sufficient knowledge of the incident. Elevating urgency over knowledge or understanding of the incident increases the risk that disclosures may be erroneous. Having many prompt "unreliable" disclosures is therefore problematic.

information. There is also a certification required to confirm the sanitization of all relevant information.

3052.204–72 Alternate I. When Federal information systems, including contractor information systems *operated on behalf of the agency*, are used to collect, process, store, or transmit CUI, the 3052.204–72 Alternate I clause is required. This adds a requirement that contractors have an ATO, granted by DHS, before they collect, process, store, or transmit CUI within a federal information system. The ATO is valid for 3 years, unless otherwise specified, and must be renewed every 3 years. The Alternate I clause also requires a DHS security authorization process and "an independent third party [to] validate the security and privacy controls in place for the information system(s)," based on NIST SP 800-53.

Key to understanding the ATO process are separate DHS Information Technology Security Policies, such as DHS Sensitive Systems Policy Directive 4300A, the Security Authorization Process Guide, and the DHS Security Authorization Templates. Where cloud computing is involved, these anticipate use of the FedRAMP program. The ATO process, generally speaking, is not dissimilar to what is used for FedRAMP authorization, and FedRAMP is used for cloud services operated for or on behalf of federal agencies.

48 CFR 3052.204–73, Notification and Credit Monitoring Requirements for Personally Identifiable Information (PII) Incidents

The clause at 3052.204–73 is applicable to solicitations and contracts where contractor and/or subcontractor employees have access to PII. The clause requires contractors to have in place procedures and the capability to notify and provide credit monitoring services to any individual whose PII or SPII was under the control of the contractor or resided in the information system at the time of a cyber incident.

The decision to provide notification and credit monitoring services is specific to each incident. The Contracting Officer will advise contractors of their requirements depending on the incident on a case-by-case basis, and the decision will ultimately depend on the severity of the incident.[9]

VI. ASSESSMENT & KEY TAKEAWAYS

DHS published this final rule more than 6 years after it first issued the proposed rule. Over the same period, DoD has implemented and been operating under its rules for safeguarding CUI, including DFARS 252.204-7012. Compared to DFARS 252.204-7012, the DHS "safeguarding" clause (3052.204-72) has requirements that—on their face—appear similar. On closer review, however, the requirements differ significantly.

[9] For comparison, DoD includes credit monitoring services as one of the ways in which contractors may be required to mitigate the risk posed by the breach of PII. *See* DoDM 5400.11 (May 6, 2021), §7.2(b) (listing terms relating to breach response that must be included in contracts).

A. "Adequate Security"

For instance, the DHS and DoD rules both require "adequate security" sufficient to protect CUI from unauthorized access and disclosure. However, the DHS final rule has a definition of "adequate security" that is unique to DHS and lacks specificity both in process and in cyber controls. While ***DoD*** relies upon NIST SP 800-171 as the baseline for defense contractor cyber measures, ***DHS*** rejects this approach, explaining:

> DHS does not accept the recommendation to modify the scope of the rule to exclude contractor information systems or explicitly identify NIST SP 800–171 as the applicable security standard for such systems. There is a misconception among industry actors that NIST SP 800–171 is the only policy that must be followed when CUI is provided or accessed under a contract. This is not correct.

88 Fed. Reg. at 40565. As explained, this is because the DHS rule applies not to commercial, nonfederal information systems as may be used on a supply or service contract, but to Federal information systems which are "used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency." *Id.* DHS continues:

> When the Government determines that a contractor information system is being operated on its behalf, that information system is considered a Federal information system and subject to the requirements of NIST SP 800–53 …

Id. This makes sense, so long as the regulation is limited to those contractors who operate an information system on behalf of the agency. It becomes most problematic if the "adequate security" obligation of the DHS regulation is applied to other situations, e.g., to "any situation where contractor and/or subcontractor employees may have access to CUI because of their relationship with DHS." HSAR 3004.470-3(a). As to the contactors in such a situation, the regulation fails to provide any clear baseline for security controls and avoids employing NIST SP 800-171 even though it was designed by NIST, and is employed by DoD, for nonfederal information systems as contractors employ.

B. Definition of "Controlled Unclassified Information" (CUI)

Obviously, it is important to define clearly what is "CUI" for which "adequate security" must be provided under this final rule. DHS asserts that it is "fully consistent with E.O. 13556 and 32 CFR part 2002" (the NARA CUI Rule). DHS introduces a new and distinct definition of CUI, however. CUI is defined, in the Safeguarding clause at HSAR 3052.204-72(a), as:

> Controlled Unclassified Information (CUI) is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls.

The DHS rule proceeds to describe eleven categories and subcategories for specific DHS-related CUI, such as Chemical-terrorism Vulnerability Information (CVI), Protected Critical Infrastructure Information (PCII), Homeland Security Agreement Information, Homeland Security Enforcement Information, and Operations Security Information. All eleven are included in the present form of the CUI Registry that NARA maintains. The DoD CUI Program website, which now states that "[n]ot every category and authority listed in the Registry is applicable to DoD," does not include nine of the eleven CUI categories cited in the DHS rule. DHS indicated, in response to a comment previously submitted to the proposed rule, that this DHS-specific CUI definition would add onto the definitions and requirements of the government-wide CUI program developed by NARA.

As is true for DoD contractors, the ability of DHS contractors to protect CUI depends greatly on the extent to which the agency validly identifies and designates the forms of CUI that it expects its contractors to protect.

C. Required "Independent Assessment"

The new, final DHS rule requires contractors to "have an independent third party validate the security and privacy controls in place for the information system(s)." HSAR 3052.204-72(h)(1)(ii) (Alternate I). Note that this requirement ***only*** applies when Federal information systems – which include contractor information systems operated on behalf of an agency – are used to collect, process, store, or transmit CUI.

DoD's CMMC 2.0 initiative is expected to require independent third-party assessment to validate contractor satisfaction of the NIST SP 800-171 controls invoked by DFARS 252.204-7012. The DHS rule differs substantially, however: (i) it would ***not*** apply to commercial, nonfederal information systems used by companies who supply goods or services to DHS; (ii) for DHS, the cyber performance standard is NIST SP 800-53, while DoD requires satisfaction of SP 800-171; and (iii) the DHS rule has no counterpart to the CMMC program features which have established The Cyber AB and its responsibilities to train and accredit persons who are Certified CMMC Assessors (CCAs) or CMMC Third Party Assessment Organizations (C3PAOs).[10]

[10] As noted previously, the DHS Alternate I process has similarities to the FedRAMP cloud authorization process. In the Security Authorization Process Guide Version 11.1 (dhs.gov), at 18, 21, DHS recognizes that where it requires FedRAMP compliance, a Third Party Assessment Organization (3PAO) provides "documentation and testing" which decreases the time for approvals and serves to "independently verify and validate their security implementations." Elsewhere, DHS states that "[a]gency 3PAO authorizations go through a third party independent assessor." *Id.,* at 22. There is no counterpart to the accreditation mechanisms that DoD has fostered in the CMMC program.

D. Incident Reporting

The DHS and DoD rules both require incident reporting for known or suspected incidents involving PII or SPII. As elsewhere, however, there are important differences.

DoD contractors are required to "rapidly report" any cyber incident that "affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract." DFARS 252.204-7012(c). Essentially, DoD wants to know about any incidents that could impact the performance of a DoD contract or the information or information systems used by the contractor in performing the contract, and DoD is especially interested in determining whether an incident could impact a DoD mission or capability. DoD is most interested in the consequences to the Department when the confidentiality of CUI is compromised.

The new DHS rule imposes incident reporting requirement for contractors that reflect DHS Policy Directive 4300A which, relying upon FISMA, defines an "incident" as "an occurrence" that—"[a]ctually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system" or "[c]onstitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." This is a broader and different definition of "incident" than used by DoD in DFARS 252.204-7012.[11] The difference may be explained by understanding that HSAR 3052.204-72(a) governs Federal information systems, including those operated by a contractor on behalf of the agency; as such, the FISMA obligations upon agencies apply. The DHS final rule does not address what incident reporting obligations apply to commercial (nonfederal) organizations performing DHS contracts for supplies or services.

For those companies who are subject to this DHS final rule, the deadline for incident reporting is more burdensome than DoD imposes on its contractors. DHS requires incidents to be reported within only 8 hours of discovery and, for any incidents involving PII or SPII, the reporting window narrows to only 1 hour. HSAR 3052.204-72(c)(2). In contrast, DoD requires reporting within 72 hours of discovery of any incident. Contractors who operate information systems on behalf of DHS will need to develop very prompt mechanisms to satisfy the final DHS rule, especially for breaches involving PII or SPII.[12]

---

[11] A cyber incident, as defined in DFARS 252.204-7012(a), "means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein."

[12] Other agencies impose similarly rapid reporting obligations where a breach exposes sensitive personal information. For example, where a breach involves PII or Protected Health Information (PHI), the Defense Health Agency requires initial notification to several federal entities within just 1 hour, with other deadlines applicable to related notifications. DHA Guidelines for Reporting Breaches 2018 Updated.pdf.