THOMPSON HINE

Privacy & Cybersecurity Update

July 2023

New Data Security and Breach Notification Obligation for DHS Contractors

In light of persistent and pervasive high-profile data breaches involving the federal government's controlled unclassified information (CUI), the U.S. Department of Homeland Security (DHS) amended its contractor acquisition framework to "demonstrate the need to ensure that information security protections are clearly, effectively, and consistently addressed in [DHS] contracts." Specifically, a new DHS information security and data breach notification procurement rule impacting its contractors and subcontractors went into effect on July 21.

The new DHS rule adds a new clause (Safeguarding of Controlled Unclassified Information) to the Homeland Security Acquisition Regulation (HSAR) that addresses a broad range of information security requirements. Although DHS noted that "there is no 'true' way to completely prevent an incident from occurring" and "there is no such thing as an 'unhackable' system," its new rule sets forth information security requirements, including exceptionally stringent data breach notification timelines.

Background

The new HSAR rule primarily applies where private-sector contractor information systems are operated on behalf of a U.S. government entity (such as a DHS Component Agency). In such circumstances, the contractor information system is considered a federal information system and is therefore subject to the same security requirements as federal information systems. Accordingly, the new HSAR rule identifies the security and process requirements such systems must meet before they are able to operate on behalf of an applicable government agency. Importantly, the rule does not identify any security requirements or processes for information systems that are not categorized as federal information systems. In other words, the new HSAR rule "is intentionally silent" on the security requirements that may apply to nonfederal information systems, such as NIST 800-171, because such requirements are being developed through a separate regulatory process.

Data Breach Notification Obligations

The HSAR rule defines an "incident" as "an occurrence that (1) [a]ctually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) [c]onstitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."

Under the new rule, a subset of DHS contractors and subcontractors must report all known or suspected incidents to the DHS Component Security Operations Center (SOC) in accordance with Attachment F, Incident Response, to DHS Policy Directive 4300A, Information Technology System Security Program, Sensitive Systems, or if the Component SOC is not available, to the DHS Enterprise SOC. DHS subcontractors are required to notify the prime contractor that they have reported a known or suspected incident to DHS, and lower-tier subcontractors are required to likewise notify their higher-tier subcontractor until the prime contractor is reached.

In addition, the new HSAR rule requires a subset of DHS contractors to report known or suspected incidents that involve personally identifiable information (PII) and sensitive personally identifiable information (SPII) within

one hour of discovery and all other incidents (such as those impacting any other category of CUI) within *eight hours* of discovery.

PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. According to DHS, "[c]ertain data elements are particularly sensitive and may alone present an increased risk of harm to the individual," such as Social Security numbers, driver's license or state identification numbers, Alien Registration Numbers, financial account numbers, and biometric identifiers.

These DHS contractors must also provide several data elements if available at the time the incident is reported, with any remaining data elements provided within 24 hours of submitting the initial incident report, including (but not limited to):

- Location(s) of the incident
- Date and time the incident was discovered
- Server names where CUI resided at the time of the incident, both at the contractor and subcontractor level
- Description of the government PII or SPII contained within the system
- Any additional information relevant to the incident

In responding to a security incident, certain levels of DHS contractors must "immediately preserve and protect images of known affected information systems and all available monitoring/packet capture data," and such data must be retained for at least 180 days from submission of the incident report to allow DHS to request the media or decline interest. DHS may, at its sole discretion, obtain assistance from other federal agencies and/or third-party firms to aid in incident response activities.

Incident reporting required by the new HSAR clause does not in any manner rescind the contractor's responsibility for other incident reporting pertaining to its unclassified information systems or as a result of other applicable statutory or regulatory requirements or other U.S. government requirements.

Credit Monitoring Services

When data security incidents impact PII or SPII, the new HSAR rule provides that certain contractors must notify affected individual within five business days after being directed by the DHS contracting officer, or as otherwise required by applicable law. The method and content of any notification by the contractor shall be coordinated with, and subject to prior written approval by, the DHS contracting officer. However, the contractor may not proceed with notification unless directed in writing by the contracting officer.

The notification method may consist of letters to affected individuals sent by first-class mail, electronic means, or general public notice, as approved by the government. Notification may require the contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

- A brief description of the incident
- A description of the types of PII or SPII involved
- A statement as to whether the PII or SPII was encrypted or protected by other means
- Steps individuals may take to protect themselves
- What the contractor and/or government are doing to investigate the incident, mitigate the incident, and protect against any future incidents
- Information identifying who individuals may contact for additional information

The DHS contracting officer may direct the contractor to provide credit monitoring services to affected individuals for at least 18 months from the date the individual is notified and may include triple credit bureau monitoring, daily customer service, alerts provided to the individual for changes and fraud, and assistance to the individual with enrollment in the services and the use of fraud alerts. The contractor may also be required to establish a dedicated call center to assist affected individuals with respect to monitoring and enrollment processes and issues.

Certificate of Sanitization

Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise indicated in the contract, the contractor shall return all CUI to DHS and/or destroy it physically and/or logically as identified in the contract unless the contract states that return and/or destruction of CUI is not required. According to the new HSAR rule, such destruction shall conform to the guidelines for media sanitization contained in NIST SP 800–88, Guidelines for Media Sanitization. The contractor shall certify and confirm the sanitization of all government and government activity-related files and information.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Francis E. (Chip) Purcell, Jr.
202.263.4118
Chip.Purcell@ThompsonHine.com

Joseph R. Berger
202.263.4193
Joseph.Berger@ThompsonHine.com

Thora Knight
212.908.3971
Thora.Knight@ThompsonHine.com