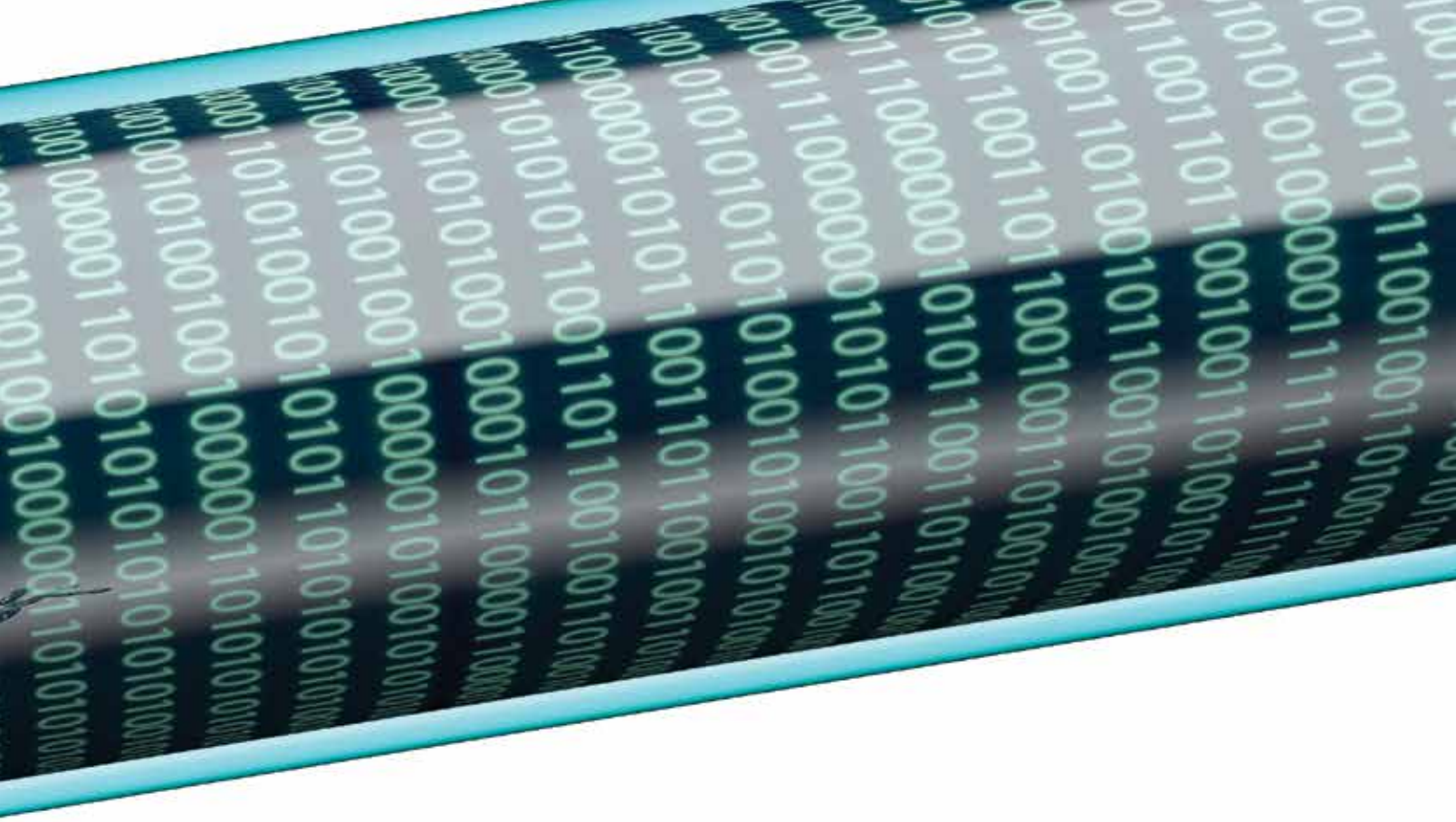
PRIVACY AND CUI: TODAY'S FEDERAL EFFORTS ARE NOT ADEQUATE TO RESPECT CITIZEN INTERESTS

By Robert Metzger



Federal regulations require departments and agencies to protect the confidentiality, integrity, and availability of information types known as "Controlled Unclassified Information" (CUI).[1] Safeguarding requirements are specified in the Federal Information Security Modernization Act (FISMA) of 2014.[2] The Department of Defense (DoD) requires its suppliers, at all tiers, to protect the confidentiality of "Covered Defense Information" (CDI), which includes all CUI categories. The National Institute of Standards and Technology (NIST) is the source of controls and enhancements used to protect CUI on federal information systems. NIST Special Publication (SP) 800-53 is the reference document for federal departments and agencies. A less rigorous set of safeguards, NIST SP 800-171, must be followed by those commercial organizations, including DoD suppliers, that are contractually obligated to protect CDI.

There are numerous types of CUI. Regulations define CUI as information that laws, regulations, or government-wide policies require to have safeguarding or dissemination controls (excluding classified information).[3] The National Archives and Records Administration (NARA) unit of the Department of Commerce maintains a "Registry" of CUI, which, today, includes twenty "Organizational index groupings" (formerly, "categories") and 122 "CUI categories" (formerly "subcategories").[4] "Privacy" is one of the twenty groupings, with eight subcategories, each of which, as defined by NARA, reference underlying federal laws, regulations, or government-wide policies.[5]

Individuals whose personal records are collected, hosted, or processed by the federal government benefit from the records' designation as CUI, where applicable, because protection is required by federal law.[6] One such law, the Privacy Act of 1974, restricts the government's collection, use, and dissemination of personal information. Under the Privacy Act, "records," as defined, may not be disclosed by the executive branch, or by any federal employee, to anyone other than the data subject or the data subject's authorized representative, "without the express written consent of the subject individual."[7] The definition of "records" is broad,[8] and the Privacy Act reaches most types of personal information that the federal government collects. The problem, as discussed in this article, is that these measures do not reach information types outside CUI categories or encompass records in the possession of commercial entities, which, by definition,

never become "records" of a federal agency. Thus, the current federal system would benefit significantly by incorporating concepts from other regimes, such as the EU's General Data Protection Regulation.

Reach of Federal Privacy Measures

Increasingly, forms of information that concern individuals or implicate their privacy interests are collected without ever being furnished to the federal government or included in a "system of records" as regulated by the Privacy Act.[9] Information generated through social media or consumer web interaction, for example, or captured through operation of autonomous sensors such as used by Internet of Things (IoT) technologies, impacts privacy and civil liberty interests of hundreds of millions of U.S. persons. In general, the scheme of federal protection of privacy information does not apply to information that is collected, hosted, or processed by commercial or other non-federal entities.

The principal purpose of the safeguarding and dissemination requirements of the CUI Rule, as well as that of the Privacy Act, is not to assure that privacy interests of individuals are protected against cyber breach (or other manipulation or misuse). Rather, the CUI Rule, the Privacy Act, and the federally required cyber safeguards are in place to enable agencies (and their employees) to comply with laws, regulations, and government-wide policies.

As practiced by the federal government today, privacy is subordinate to security. The principal purpose of FISMA, Federal Information Processing Standards (FIPS), the NARA CUI Rule, and the NIST Safeguards, as well as that of current federal security regulations applicable to contractors, is to assure that federal agencies protect the confidentiality, integrity, and availability of information types where this is required by operation of federal law, regulation or government-wide policy.[10]

The Privacy Act has limited application to government contractors or to other non-federal entities to whom forms of CUI may be shared and entrusted. If a contractor operates "systems of records" containing personal information, the Privacy Act applies. Similarly, a contractor and its employees are considered employees of a federal agency, and subject to the same safeguarding requirements as federal employees, when an agency contracts for the design, operation, maintenance, or use of systems containing information covered by the Privacy Act.[11] In the same vein, a private contractor that operates an information system "on behalf of" the federal agency may be subject to the Privacy Act as well as other obligations, to protect CUI, as apply to that agency under the CUI Rule.[12]

Across the broad federal landscape, however, there are many thousands of private companies, and other non-federal entities, who may receive one or another form of information, from a federal agency, that concerns the privacy interests of individuals, but that is not covered by the Privacy Act and not subject to the CUI Rule. Only if the non-federal entity operates a "system of records" for a federal agency or uses or operates an information system "on behalf of" a federal agency do the full range of federal protections apply. Per NIST SP 800-53, these encompass measures to secure "confidentiality," "availability," as well as "integrity" of the information. As to commercial companies that may receive CUI, such as a DoD contractor, the applicable NIST standard, SP 800-171, protects only "confidentiality."

As suggested by the painful experience of the Office of Personnel Management (OPM) breach, where 21.4 million personal records were compromised, federal safeguards are less than perfect even as to systems subject to full SP 800-53 requirements. Corresponding safeguards do not apply to CUI in the Privacy categories when provided to or created by federal contractors or other non-federal entities. And for the much larger universe of commercial companies that host, process, transmit, or use information of these and other sensitive types, federal cyber safeguarding requirements are absent altogether.

Considering the ever-expanding volume of information where individuals have a privacy interest, present federal protections, at their best, barely scratch the surface. There is no general federal requirement that any commercial entity protect the privacy of even those forms of information, which, if held by a federal agency, would qualify as "CUI" or be subject to the Privacy Act requirements.

Beyond the absence of required protection, as to many information types, individuals whose personal and privacy interests are exposed too often are uninformed entirely, about the collection of information and its use, or receive meaningless "notice" followed by uninformed "consent."

This should change. Looking backward, cyber breaches that compromise sensitive forms of personal information have occurred for years, all too often at massive scale, and with little evidence that threats have abated, vulnerabilities have been mitigated, and consequences avoided. And today, such "remedies" as exist to protect the personal interests of individuals affected are largely confined to "breach notification" obligations. Even these are not now required by federal law but arise as a function of a patchwork of state measures. The primacy of state laws in this area is anachronistic. There is rarely (if ever) any relationship between any state boundary and the architecture of an information system that stores or processes personal information.[13]

Breach notification measures offer little assurance and dubious value to those who may be notified after their

Robert S. Metzger *(rmetzger@rjo.com) is a shareholder of Rogers Joseph O'Donnell, PC, a law firm that has specialized in public contracts for more than 35 years. He heads the firm's Washington, D.C. office and counsels leading U.S. and international technology firms. He is active in public-private initiatives involving cyber and supply chain security.*

personal records suffer a breach. Notice of a breach, by definition, occurs after the adverse event, does not recover information lost by the breach, and informs no one as to the responsibility—or the culpability—of the breached enterprise. While a breached entity is not the initiator of the attack that produced the event, in today's environment every company holding valuable technical information or entrusted with personal records owes the owners and data subjects an obligation of due care to possess and maintain adequate security in a dangerous, dynamic environment. Breach statutes that generate notices are a palliative remedy only. When delivered after the fact, the subject of actual or threatened injury learns of the event and about personal exposure but knows nothing of the condition that led to the loss or whether the affected enterprise has taken corrective measures to close the vulnerability to protect against recurrences of the breach.

The IoT as a "Forcing Function"

With the Internet of Things (IoT) era fully upon us, the hazard to privacy interests is growing exponentially. There are many variations of IoT functionalities. Some of these involve the massive deployment of sensor-enabled networks collecting huge quantities of data arising from or relating to the personal conduct of individuals. There is no assurance whatsoever that individuals whose data are harvested from IoT devices, are even aware of what systems collect information from or about them, or how, by whom, or for what that information is used—much less that these individuals have approved such collection or use. Further, a populace kept ignorant of the collection of its personal data is not informed of whether or how their data are protected.

IoT-collected data about individuals—their habits, interests, travel, action, exercise, location, etc.—is not the "property" of the collector or processor of such information, even if it is their instrumentalities that create, harvest, or exploit those data. No one should be under any illusion about the "exo-scale" threat to privacy posed by the IoT. This is not even a case where information of a user's choice is shared under some "notice-and-consent" scheme, as happens with many web interactions or in some social media use cases. Rather, IoT sensor regimes—of which there are more every day, and virtually everywhere—collect massive amounts of personal data of many types without, in many cases, even the possibility that the affected individual is aware of the collection, transmission, processing, application, or disposition. The individual, similarly, is exposed to adverse personal consequences should a security breach occur, even though she or he may never have had a clue that information about him or her was being collected by persons—or "things."

The federal government, as explained, goes to some lengths to protect certain defined categories of information, CUI, on federal information systems—i.e., those operated by federal agencies or by non-federal entities on their behalf. By operation of regulation or contract term, similar measures are imposed upon a relatively small number of government contractors or other non-federal partners. None of these measures—modest though they are—protect individuals against the misuse, compromise, or loss of personal information about them that is or will be collected by or for the government using IoT instrumentalities.

In the few areas of government business where it now requires commercial companies to provide any form of cyber safeguard for CUI, including the Privacy categories, neither the reach nor the result of such measures addresses the scale or diversity of IoT-collected and generated information of significance to individuals. What is more, the nature of protections, for users and use cases subject to federal requirements, does not require even elemental security measures to achieve and sustain privacy for the millions of individuals about whom IoT, sensor-driven networks are generating troves of information. Existing

With the Internet of Things (IoT) era fully upon us, the hazard to privacy interests is growing exponentially.

cyber controls protect just those information types that qualify as CUI, and only on those information systems that are operated by federal agencies or by contractors "on behalf of" agencies. Nothing in contemporary statutory or regulatory obligations, or government-wide policy, even contemplates, much less protects, new information types, as collectable through the IoT, that can be used or abused to affect, impair, or injure the personal privacy interests of individuals.

The GDPR Is a Different Paradigm

The General Data Protection Regulation (GDPR) became effective in May 2018. It applies to the processing of personal data of subjects residing in the European Union (EU), regardless of where the processing of the data takes place or the location of the company with custody over the data. [Art. 3] U.S. and multinational companies may be subject to the GDPR and, at the same time, other privacy and security requirements. By comparison to the United States, the relationship between privacy and security, in the EU, under the GDPR, and the importance of the individual, as opposed to the organization, differ profoundly.

The present federal regime for protection of CUI has a primary compliance objective, for the organization, with some protection of individual privacy as an included but subordinate benefit. The GDPR seeks protection of privacy—and security is a means to achieve that goal.

The subject of the GDPR is "personal data." It is defined generously:

> "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. [Art. 4]

The GDPR, at Article 4, provides an expansive definition of the "personal data" that impose obligations on enterprises that are "controllers" or "processors" and that are to be protected and subject to many enumerated individual rights. There are further and more detailed definitions of more specialized terms, e.g., "'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."

Fits and Misses Between CUI Protection and the GDPR

There is some overlap to the types of CUI in the NARA Registry and the categories of "personal data" protected under the GDPR. Privacy interests covered by the GDPR can be associated to the following CUI categories and subcategories, e.g., Financial (Electronic Funds Transfer, Net Worth, Retirement); Law Enforcement (Criminal Records History, Financial Records); Privacy (Contract Use, Genetic Information, Health Information, Personnel, Student Records). In every case, the CUI definitions are written not to cast a "broad net" to capture the interests of the actually affected individual(s), but to conform to specific federal laws, regulations, or government-wide policies.

The GDPR also takes a completely different approach. The GDPR is agnostic to technologies and endorses no specific or control regime. The GDPR is "strategic" and seeks to achieve high-level privacy objectives that have no generally applicable U.S. counterpart:

- **The GDPR includes a right of erasure**—also called the "right to be forgotten." For this purpose, a data controller "shall take *reasonable steps*, including technical measures." [Art. 19]
- **The GDPR requires security of processing**, which involves "technical and organisational measures appropriate to risk." [Art. 32]
- **The GDPR requires an "impact assessment,"** which calls for "security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance." [Art. 35]

The GDPR imposes obligations upon data processors and controllers to "implement appropriate technical and organisational measures to ensure" compliance. [Arts. 24, 25, 28, 32] The GDPR is silent on methods, standards, and practices. Instead, the emphasis is upon discrete objectives, and it is the responsibility of data controllers and processors to select and implement technical measures sufficient to achieve these ends. As the GDPR aims to protect those in the EU from privacy abuses and data breaches, information security is not an end in and of itself. Rather, it is among the means considered necessary to protect the privacy rights and expectations of individual(s) whose data are utilized by enterprises of any type—not just governments or their contractors.

The GDPR does not direct the use of particular security measures. It does not endorse any standards or recommend adherence to identified "best practices." However, enterprises are motivated to achieve security because they are subject to potentially very large fines—the greater of 20 million euros or 4% of global revenue per infraction—for "infringements." [Art. 83] When a "supervisory authority" determines the amount of fine to apply to an individual case, "technical and organizational measures," implemented pursuant to Articles 25 and 32, are just some of many considerations.

Even as to that "sub-universe" of companies to whom the U.S. government requires measures for CUI security and Privacy Act compliance, the approach is far more prescriptive. U.S. requirements obligate federal contractors to adopt and implement enumerated "safeguards," "controls," or "enhancements," as are invoked by regulation or imposed by contract. The focus is upon process as the means to

achieve the desired results. The EU approach, in contrast, is on the results. A subject company could be exposed to substantial administrative fines under the GDPR where a damaging breach occurs even if that company can document technical adherence to one or another established set of standards or best practices. In the United States, unfortunately, many regulated companies seek the least costly, "minimalist" approach to technical compliance. A breach may produce controversy, or trigger incident response or other notification obligations, but there is nothing remotely resembling the prospect of very large fines as can be imposed by EU supervising authorities. Presumably, the exposure to such liability motivates GDPR-subject companies to continuing vigilance in the selection and enhancement of security measures. Also, under Article 83 of the GDPR, actions taken by the enterprise "to mitigate the damage suffered by data subjects" can be a factor in the amount of the fine, as can "the manner in which the infringement became known to the supervisory authority." Use of technologies to monitor networks and information systems, such as continuous diagnostics and mitigation (CDM), could reduce the risk and limit the scope of breach, and expedite knowledge and remediation.

Federal agencies and their contractors are required to establish security using specified standards and controls. Under FISMA, contractors that operate systems "on behalf of" federal agencies must implement controls specified by NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations).[14] Some government contracts require commercial organizations to protect CUI if provided by the government or created by a company for the government. A DoD contract clause, applicable to the entire defense supply chain, requires contractors to have "adequate security" employing NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations).[15] SP 800-171 describes 110 individual safeguards allocated into fourteen security families. Each of the safeguards is expressed in a single sentence, but, as applied by DoD, every contractor subject to the CUI protection obligation—at any level, regardless of the nature or sensitivity of their work, and irrespective of their resources or the uses they make of CUI information—must conform to every one of the 110 safeguards unless relief is sought and obtained from a government authority.

Although the GDPR contains no details whatsoever on methods, standards, safeguards, controls, or enhancements, it is accompanied by both strong sanctions and a means of enforcement by EU member states. For U.S. suppliers, CUI protection obligations apply only by operation of a contract clause, not by a plenary statute, and many contractors understand the contract term to make it the responsibility of the government to identify or designate such CUI as may be in the contractor's possession and subject to protection. By comparison, the GDPR applies to anyone that meets the definition of a "data processor" or "controller" and to any "Personal Data" (as defined) of any identifiable natural person.

The U.S. methods, even if characterized as "informative" rather than "prescriptive," are confining and normative, while the GDPR approach is performance-oriented, more flexible, and certainly more accommodating of risk-based decisions and of tailoring to individual circumstances of regulated enterprises. At Article 83, for example, the GDPR states that in determining the amount of administrative fines, a supervisory authority shall take into account, among other factors, "the nature, scope or purposes of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them."

There is no effective or demonstrated enforcement mechanism of U.S. contract requirements to safeguard CUI. Contractual oversight is presently limited. Contractual security clauses are rarely enforced. Rarely has the federal government sought damages from a contractor

Rarely has the federal government sought damages from a contractor that failed to fulfill security requirements.

that failed to fulfill security requirements. And, if it did, damages would be difficult if not impossible to quantify, and any damages recovered would inure to the benefit of the government, not any individuals whose data are compromised.[16] This is a far cry from the GDPR, which states, at Article 82, that *any person* who has suffered "material or non-material damage" as a result of infringement of the GDPR "shall have the right to receive compensation from the controller or processor for the damage suffered."

Correlations between the GDPR and U.S. measures to protect CUI are neither direct nor clearly mapped. This presents many companies with a serious quandary. Neither the GDPR nor the CUI regime exists in isolation from one another—even though their "fit" is problematic. To the contrary, many companies, based in the EU and otherwise, are subject to the GDPR, as concerns personal data they collect or process for EU persons, as well as subject to U.S. CUI requirements, where they or affiliates are under a federal contract imposing the NIST safeguards.

Some companies will be able to create information systems, policies, and practices that are distinct and different, for performance of U.S. contracts subject to CUI protection, on the one hand, and to satisfy the GDPR, on the other. But this will be neither practical nor affordable for many companies. Accordingly, it is important to establish means to reconcile the respective regimes. This is *especially* important because U.S. federal civilian agencies are now working to complete rule-making by which CUI protection measures, like those now imposed upon DoD's suppliers, will be extended to civilian agency contractors and other non-federal CUI recipients. Preliminary estimates are that many *hundreds of thousands* of U.S. companies, most presently unaware of the prospect, will become subject to contractual CUI protection mandates once the new rule is final. Even less well understood is the extent to which many of these same entities, and thousands of others, are likely to have obligations, by operation of the GDPR, to protect personal information of persons (as may be their employees, customers, or others) in the EU.

Protection of Privacy in the U.S. Requires a Change of Strategy and Practice

There are difficult choices to be made. Should the U.S. elevate privacy as a fundamental interest to be protected by all governmental and commercial entities, requiring (as does the EU) security as one among many measures to respect privacy? Should this be done by federal statute or new, broadly applicable regulations? Many commercial enterprises undoubtedly would resist, especially those holding a market-driven business premise that they own the new forms of data that concern individuals which they collect and process. Opposing this "proprietary" theory is the public policy proposition that every individual should possess the right to know and determine who may have, use, or otherwise exploit information from or about them and that, as in the EU, all data controllers or processors should face liability for failure to fulfill privacy requirements, inclusive of security of information rightfully obtained.

The federal government today does not use its regulatory power to require the general protection of privacy. Only on a limited basis does it require holders of Privacy CUI to have security measures to protect that information. The CUI definitions of privacy, each rooted in laws, regulations, or government-wide policies, may be too narrow. Individuals have privacy interests in many forms of information that are presently unregulated. U.S. persons are subject to an ever-expanding variety of data collection methods. U.S. persons are subject to undisclosed or unauthorized data collection or processing, and even sale (or "brokering") of such personal data is largely unregulated. The *collection* and *processing* of non-regulated forms of information is generally done without the knowledge of the data subjects, without their consent, and without any assurance that such information about them will be subject even to elemental security protection. The neglect of privacy considerations, coupled with the absence of security, is an invitation to manipulation, abuse, and injury—potentially affecting millions of Americans.

Information system security, without respect for and preservation of privacy, can be said to elevate the interest of the enterprise (government or commercial) above that of the individual. The IoT shows vividly how the pursuit of new markets and commercial opportunity can far outpace what citizens know or understand of how innovative technologies capture and exploit personal information. There are important reasons for the federal government to separate and elevate privacy as an objective not incidental to the preservation of federal information but as a central principle of how the federal government can protect the rights and liberties of its citizens. The United States may take a different tack from the GDPR, but there is much to be learned from study of the EU experience. Efforts should be made to develop internationally accepted strategies and practices. ◆

Endnotes

1. *See* Executive Order (E.O.) 13556, Controlled Unclassified Information (Nov. 4, 2010), *available at* http://www.whitehouse.gov/the-press-office/2010/11/04/executiveorder-13556-controlled-unclassified-information. The E.O. states as its purpose to "establish a uniform program for managing information that requires safeguarding or dissemination controls." The National Archives and Records Administration (NARA) is the Executive Agent assigned to implement E.O. 13556. Circular No. A-130 establishes the federal government's information management policy. One attribute of that policy is to "[p]rotect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information." OMB Circular A-130, 8.a(g), *available at* http://www.whitehouse.gov/omb/circulars_a130. The Department of Defense has issued its own Manual regarding treatment of CUI. *See, e.g.*, DoD 5200.01, Vol. 4 (DoD

Information Security Program: Controlled Unclassified Information (CUI)), *available at* https://www.dodig.mil/Portals/48/Documents/Policy/520001_vol4.pdf.

2. 44 U.S.C. §§ 3551 et seq.

3. *See* 32 C.F.R. § 2002.1(c). The "Controlled Unclassified Information" final rule (the "CUI Rule"), 32 C.F.R. Part 2002, may be found at 81 Fed. Reg. 63,324 (Sept. 14, 2016).

4. *Controlled Unclassified Information (CUI)*, Nat'l Archives, https://www.archives.gov/cui/registry/category-list.

5. Subcategories include subjects such as "general privacy," "genetic information," and "health information." The "General Privacy" subcategory, *e.g.*, *available at* https://www.archives.gov/cui/registry/category-detail/privacy.html, references two federal statutes, eleven federal regulations, and two OMB Circulars as authority for safeguarding and/or dissemination control.

6. "FISMA requires federal agencies to implement a mandatory set of processes and system controls designed to ensure the confidentiality, integrity, and availability of system-related information." GSA 2012 Agency Financial Report, Federal Information Security Management Act, *available at* http://www.gsa.gov/portal/content/150159. The processes and system controls in each federal agency must follow established Federal Information Processing Standards (FIPS), NIST standards, and other legislative requirements pertaining to Federal information systems, such as the Privacy Act of 1974, 5 U.S.C. § 552a. Privacy Act regulations, issued by the Office of Personnel Management (OPM), are available at 5 C.F.R. §§ 297.101 et seq.

7. 5 U.S.C. § 552a(b); 5 C.F.R. §297.102.

8. The term "record" means "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." 5 U.S.C. § 552a(a)(4).

9. The Act defines "system of records" as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." *Id*. § 552a(a)(5). The basic obligation of agencies to respect individual privacy applies to "records" that are "contained in a system of records." *Id*. § 552a(b).

10. To a lesser degree, these agency regulations also operate to shield agency employees involved in the handling of this information from exposure to criminal penalties under the Privacy Act of 1974. *Id*. § 552a(i).

11. *See, e.g.*, *Privacy and Contract Requirements,* Gen. Serv. Admin., *available at* https://www.gsa.gov/reference/gsa-privacy-program/privacy-and-contract-requirements.

12. As explained in the promulgation comments accompanying the NARA CUI Rule, "'on behalf of' means when a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting federal information, and those activities are not incidental to providing a service or product to the Government." To protect such systems and information, agencies must prescribe appropriate security requirements and controls from FIPS Publication 200 and NIST SP 800–53 in accordance with any risk-based tailoring decisions they make." 81 Fed. Reg. 63,330 (Sept. 14, 2016).

13. There is no federal "breach notification" statute. In June 2015, OPM announced that it had been breached and that as many as 21.5 million records, of federal employees as well as contractor personnel, had been compromised. *See* https://www.opm.gov/cybersecurity/cybersecurity-incidents/. Subsequently, the Office of Management and Budget (OMB) issued a new breach response policy, Memorandum M-17-12, for federal agencies, setting minimum standards with respect to personally identifiable information (PII). Federal breach notification legislation has been introduced and debated in Congress since 2006 without ever seeing even one of nineteen distinct measures getting to a floor vote in either house of Congress. In 2018, South Dakota and Alabama became the last of the 50 U.S. states to adopt a state-level "breach notification" statute. Caleb Skeath & Brooke Kahn, *State Data Breach Notification Laws: 2018 in Review*, Inside Privacy (Dec. 31, 2018), https://www.insideprivacy.com/data-security/data-breaches/state-data-breach-notification-laws-2018-in-review.

14. SP 800-53 Revision 4 is currently applicable. NIST is nearing completion of Revision 5 which will elevate the importance of privacy controls. Specifically, NIST advises that Revision 5 will make security and privacy controls more outcome-based and that privacy controls will be fully integrated into the security control catalog, creating a consolidated and unified set of controls. When implemented, these will be important measures. Also positive is that NIST intends Revision 5 to be useful to a broad base of public and private sector organizations. Only federal organizations, and contractors operating systems on their behalf, are required to implement controls drawn from SP 800-53, however.

15. The DFARS clause, at 48 C.F.R. § 252.204-7012 ("Safeguarding covered defense information and cyber incident reporting") is used by the DoD to impose CUI security measures upon its contractors, and that obligation "flows down" to all levels of the supply chain. Compliance with the –7012 clause is achieved by implementation of the 110 safeguards stated by NIST SP 800-171.

16. In the OPM breach of 2015, records of extraordinary sensitivity (including security clearance investigations) were lost, but OPM did not seek to recover damages from the contractor that was responsible (according to some press reports). Lawsuits were brought by public employee unions against OPM and a contractor alleged to be responsible for the breach, but these were dismissed by a lower court and now are on appeal to the D.C. Circuit Court of Appeals. *In re* U.S. Office of Personnel Mgmt Data Sec. Breach Litig., Nos. 17-5217 & 17-5232.