Technology Policy Update
27 March 2020
By Michael Kans, Esq.

Moran Releases Long Awaited Privacy Bill Without Blumenthal

Senator Jerry Moran (R-KS) has released his long-awaited privacy and data security bill, the "Consumer Data Privacy and Security Act of 2020" (S.3456) that is not cosponsored by Senator Richard Blumenthal (D-CT) even though the two Senators have been in talks since late 2018 along with other Senators to draft a bipartisan bill. Of course, Moran chairs the Senate Commerce, Science, and Transportation Committee's Manufacturing, Trade, and Consumer Protection Subcommittee and so is a key stakeholder with input on any privacy and data security legislation coming from that committee. However, Moran's bill is likely a nonstarter with Senate and House Democrats because it does not provide people with a private right of action and it would preempt state laws like the "California Consumer Privacy Act" (CCPA) (AB 375). Moreover, the Federal Trade Commission's (FTC) ability to obtain civil fines would be limited only to situations where the entity in question had actual knowledge of the violations as opposed to the standard many agencies use to enforce: constructive knowledge (i.e. knew or should have known.) This, too, is contrary to not only the Democratic privacy bills but also some of the Republican bills, which would allow the FTC to levy fines on the basis of constructive knowledge.

However, like almost all the other bills, the "Consumer Data Privacy and Security Act of 2020" would require covered entities to obtain express affirmative consent to collect from and process the personal data of people after providing extensive disclosure and notice about who and with whom their personal information would be shared. Likewise, this bill would give people certain rights, such as a right to access, correct, delete, and port their personal data. People would also be granted the right of erasure under which a covered entity must delete or de-identify the personal data of any person who submits a verified request. However, small businesses would be exempted from from granting requests to access and the right to correct. There are, again like many other privacy bills, circumstances under which a covered entity may decline to grant a request to exercise these rights. For example, if doing so would violate a law or legal process, then the covered entity could say no to a person. Likewise, if a person's life is in imminent danger, then a request could also be denied. There are other such circumstances, some of which privacy and civil liberties advocates will assert will turn out to be such wide loopholes that the rights will cease to be meaningful as they have with some of the other bills.

In terms of who would be subject to the Act, entities covered by the bill would be those currently subject to FTC jurisdiction and non-profits and common carriers. Moreover, the bill has fairly expansive definitions of "personal data" and "sensitive personal data," like many of the other bills.

Like some of the privacy bills, large covered entities would have additional privacy obligations and responsibilities. For those entities that collect and process the personal data of 20 million or more people per year or the sensitive personal data of 1 million or more a year, then these entities must have a privacy officer to advise the entity on compliance and monitoring. Also, these large entities must also take extra steps for making material changes to their privacy policies, including privacy impact assessments and the development and implementation of a comprehensive privacy policy.

The Consumer Data Privacy and Security Act of 2020 tracks with other privacy bills in requiring that covered entities must also implement data security safeguards to protect the integrity, confidentiality, and security of personal data. There would be a sliding scale of sorts with less sensitive data requiring less rigorous protection and conversely the more sensitive the data, the more stringent the safeguards that must be used. Covered entities must also conduct periodic, regular risk assessments and then remediate any turned up risks. Covered entities must also ensure their service providers and any third parties with whom they are sharing personal data are instituting data security standards but at a lower defined standard than the covered entity itself. For example, the latter entities must only protect the security and confidentiality of the information they hold, collect, or process for a covered entity and are not responsibility for the integrity of the information.

When a covered entity uses a service provider to collect or process personal data, it must use a binding contract and perform due diligence to ensure the service provider has the appropriate procedures and controls to ensure the privacy and security of personal data. The covered entity also has the responsibility to investigate the service provider's compliance with the act if a reasonable person would determine there is a high probability of future non-compliance.

As noted, the FTC would be the federal enforcer of the Act under the rubric of its current Section 5 powers to seek a range of injunctive and equitable remedies to punish unfair and deceptive practices. The FTC would also be able to seek civil fines of up to $43,530 per violation but only for knowing violations, and there is no language for adjusting the per violation fine amount for inflation, a power the FTC otherwise has. State attorneys general could enforce the Act just as the FTC could.

The bill expressly preempts state laws on privacy and data security and makes clear that state laws may not interfere with HIPAA, Gramm-Leach-Bliley, FERPA, and others. Moreover, the "Consumer Data Privacy and Security Act of 2020" would not affect federal privacy laws like Gramm-Leach-Bliley, COPPA, FCRA, and others, and if entities currently subject to those federal laws are in compliance with the privacy and data security requirements, then they will be deemed in compliance with the Act.

OMB Spells Out How Agencies Should Accommodate COVID-19 Caused Contract Issues and How Technology Can Help During The Crisis

The Office of Management and Budget (OMB) has released a memorandum, "Managing Federal Contract Performance Issues Associated with the Novel Coronavirus (COVID-19)," which explains "steps to help ensure [the health and safety of all Americans] while maintaining continued contract performance in support of agency missions, wherever possible and consistent with the precautions issued by the Centers for Disease Control and Prevention (CDC)." This memorandum was issued to agencies and discusses performance of federal contracts with respect to telework, reporting to federal facilities if necessary, valid reasons for not performing a contract in a timely fashion, and possible procurement flexibility.

OMB stated that

- As the impact of COVID-19 continues to evolve, many Federal government contractors that ordinarily work side-by-side with the Federal workforce may currently be unable to access their Federal work sites as a result of building closures, quarantines or implementation of social distancing practices. Agencies are urged to work with their contractors, if they haven't already, to evaluate and maximize telework for contractor employees, wherever possible.

Telework is an important tool for enabling continued contract performance in a manner that can meet health and safety guidelines from the CDC and State and local public health authorities.

- Equally important, agencies should be flexible in providing extensions to performance dates if telework or other flexible work solutions, such as virtual work environments, are not possible, or if a contractor is unable to perform in a timely manner due to quarantining, social distancing, or other COVID-19 related interruptions. Agencies should take into consideration whether it is beneficial to keep skilled professionals or key personnel in a mobile ready state for activities the agency deems critical to national security or other high priorities.
- Additionally, agencies should also consider whether contracts that possess capabilities for addressing impending requirements such as security, logistics, or other function, may be retooled for pandemic response consistent with the scope of the contract.
- Finally, agencies are encouraged to leverage the special emergency procurement authorities authorized in connection with the President's emergency declaration under section 501(b) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. §§ 5121-5207 (the "Stafford Act"). These flexibilities include increases to the micro-purchase threshold, the simplified acquisition threshold, and the threshold for using simplified procedures for certain commercial items, all of which are designed to reduce friction for contractors, especially small businesses, and the government and enable more rapid response to the many pressing demands agencies face. The availability of these flexibilities does not mean they will always be suitable, and agencies should exercise sound fiscal prudence to maximize value for each taxpayer dollar spent. At the same time, the acquisition workforce should feel fully empowered to use the acquisition flexibilities, as needed, consistent with good business judgment in response to this national emergency.

OMB structured the memorandum in a question and answer format, and here are the most relevant excerpts:

> Should agencies be directing their Federal contractors to follow the lead of the Federal Government in their use of telework for their contract employees as described in OMB Memoranda M-20-13 and M-20-15, which discuss the use of telework in connection with COVID-19?
>
> The Federal Government's telework law and recent announcements cover only Federal managers and employees, not contractors or their employees. Federal contractors are responsible for managing their workforces, including how telework is used by their employees, consistent with their own telework policies and the contract terms they have negotiated with Federal agencies. However, in the spirit of OMB's guidance, which seeks to maximize the use of telework, and FAR § 7.108, which instructs agencies not to discourage contractor use of telework when consistent with contractual requirements, agencies are strongly encouraged to work with their contractors to evaluate and maximize telework for their contractor employees, wherever possible, as a way to enable continued contract performance consistent with the health and safety of their contractor and government personnel. This includes modifying contracts that do not currently allow for telework. If a contract does not lend itself to telework, for example, because it must be performed at a government facility, agencies should consider being flexible on delivery schedule contract completion dates.

If contractor personnel must be quarantined due to exposure to the virus, whether ·or not related to performance of the contract, and this action results in a slip in the contract schedule, may contracts be extended or otherwise altered?

Yes. Government contracts provide for excusable delays, which may extend to quarantine restrictions due to exposure to COVID-19. For example, see FAR clauses 52.249-14, 52.212-4(±), and 52.211-13. In determining the best course of action, the contracting officer should discuss the situation with the contractor to determine if other options are available (e.g., ability of employee to telework or to find a substitute employee). If other options with the existing contractor aren't feasible, it may be appropriate to re-procure elsewhere if possible. Such actions should be taken for the convenience of the government (e.g., through use of the relevant convenience termination clause or a no-cost settlement) and without negatively impacting the contractor's performance rating. Excusable delays that result in adjustments to the contractor's delivery schedule should not negatively impact a contractor's performance ratings.
Agencies are encouraged to be as flexible as possible in finding solutions.

OMB posed the question as to whether there are "special emergency procurement flexibilities of FAR §18.202 available for use in addressing requirements connected to COVID-19?" with this answer: Yes. The President has declared a national emergency concerning the novel coronavirus disease under the Stafford Act. As a result of this emergency declaration, the flexibilities identified in FAR§ 18.202, "Defense or recovery from certain events," are available for use in supporting response efforts to COVID-19. These flexibilities include increases to the micro-purchase threshold, the simplified acquisition threshold, and the threshold for using simplified procedures for certain commercial items. Specifically-
(1) The micro-purchase threshold is raised from $10,0001 to $20,000 for domestic purchases and to $30,000 for purchases outside the U.S.;
(2) The simplified acquisition threshold is raised from $250,0002 to $750,000 for domestic purchases and $1. 5 million for purchases outside the U.S.; and
(3) Agencies may use simplified acquisition procedures up to $13 million for purchases of commercial item buys.

In conducting acquisitions to support response efforts, agencies are expected to use sound fiscal prudence to maximize value for each taxpayer dollar spent. The availability of the flexibility does not mean it must be used, but agencies should feel fully empowered to use the acquisition flexibilities, as needed, consistent with good business judgment in response to the national emergency.

OMB has also released a memorandum to guide agencies in expanding their current uses of technology to execute their missions and to help them establish new means of doing so consistent with exitsing policies and programs. This memorandum, titled "Harnessing Technology to Support Mission Continuity," flows from M-20-16, "Federal Agency Operational Alignment to Slow the Spread of Coronavirus," issued last week directing agencies and departments to "take appropriate steps to prioritize all resources to slow the transmission of COVID-19, while ensuring our mission-critical activities continue." Building on that directive, OMB Deputy Director Margaret Weichert issued this document to drive greater use of technology during COVID-19 to continue agency operations, including the expansion of agency websites for public facing activities, greater use of available technological means inside each agency, and aligning these efforts with cybersecurity

and privacy considerations. However, it must be stressed that the bulk of these directives rely on existing, established initiatives and efforts, and it is mostly calling for wider implementation.

In the introduction, Weichert stated

- Over the past several years, agencies have been making significant investments in technology infrastructure, scalable technology platforms and digital delivery of mission support and mission delivery functions. In some situations, although technical capabilities are available, agency business processes have not evolved to fully utilize these expanded capabilities. By aggressively embracing technology to support business processes, the Federal Government is better positioned to maintain the safety and well-being of the Federal workforce and the American public while supporting the continued delivery of vital mission services.
- In response to the national emergency for COVID-19, agencies are directed to use the breadth of available technology capabilities to fulfill service gaps and deliver mission outcomes.

Like other recent OMB memoranda, the substance of the guidance is structured as a Q and A:

> 1. What flexibilities do agencies have to adjust operations to support mission delivery?
> OMB issued M-20-16, which provides an overarching directive with broad latitude to provide maximum flexibility to agency leaders.
>
> 2. How should agencies confirm that both internal users, and the public are positioned to leverage an agency's digital service offerings?
> Agencies are encouraged to update their .gov websites to the greatest extent practicable to provide agency service delivery information to Federal Government consumers and to direct Federal Government consumers to the appropriate digital and telephonic resources to obtain needed services. We also encourage agencies to assess the usability of its digital resources, and to improve user centered design and customer service aspects of its websites, web applications, and other citizen-facing interfaces.
> Additional Resources:
>
> - OMB M-17-06, Policies for Federal Agency Public Websites and Digital Services
> - Guidance on building better digital services in Government, https://digital.gov/resources/
>
> 3. What can agencies do to better facilitate personnel productivity in a remote environment?
> Agencies are encouraged to leverage agency approved collaboration tools and capabilities to the greatest extent practicable. This action may include increasing the number of licenses available, leveraging services and technologies across the enterprise, and directing specific activities to be conducted via collaboration forums. Additionally, it is recommended that agencies make use of collaboration tools and capabilities offered by other Federal agencies to meet capability gaps. Such use cannot override legal terms of service.
>
> Additional Resources:
>
> - Federal-Compatible Terms of Service Agreements
> - List of free tools that have federally-compatible negotiated Terms of Service
> - General Services Administration's (GSA's) Consolidated Federal Supply Schedule offers pre-negotiated terms of services agreements

Are agency cybersecurity and privacy requirements still applicable/what are some areas of focus?

Security protocols, requirements regarding the appropriate use of federal resources, and legal requirements are always applicable. However, agencies are encouraged to make risk-based decisions as appropriate to meet mission needs as outlined in M-20-16. Areas of increased focus concerning cybersecurity and privacy include:

- Updating Virtual Private Network components, network infrastructure devices, and devices being used to enable remote work environments with the latest software patches and security configurations;
- Providing guidance to employees about how to ensure proper information security and privacy controls are in place when working from alternate locations or home;
- Continuing to prohibit the unauthorized forwarding of Federal Government business materials or other information to personal devices;
- Continuing to prohibit the unauthorized usage of social media platforms or any unauthorized devices for Government business; and
- Confirming that the expanded usage of technology tools is in accordance with appropriate legal considerations and does not violate legal terms of service.

Additional Resources:

- M-13-10, Antideficiency Act Implications of Certain Online Terms of Service Agreements
- Alert (AA20-073A): Enterprise VPN Security
- GSA's Consolidated Federal Supply Schedule offers pre-negotiated terms of services agreements
- GSA's Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SIN) provides rapid access to key support services from technically evaluated vendors

CISA and NIST Release Guidance Documents To Help Determine Essential Operations and Transition To Telework

Two federal agencies have released or repackaged existing guidance to help organizations cope with telework and its attendant challenges, especially the owners and operators of critical cyber infrastructure. The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) has drafted guidance to help governments and private sector entities determine which functions and employees might be considered essential, and the National Institute of Standards and Technology (NIST) is repackaging previously released guidance on telework considerations and security.

CISA has developed and released "an initial list of "Essential Critical Infrastructure Workers" to help State and local officials as they work to protect their communities, while ensuring continuity of functions critical to public health and safety, as well as economic and national security." CISA claimed that "[t]he list can also inform critical infrastructure community decision-making to determine the sectors, sub-sectors, segments, or critical functions that should continue normal operations, appropriately modified to account for Centers for Disease Control (CDC) workforce and customer protection guidance." CISA stated that "[t]he attached list identifies workers who conduct a range of operations and services that are essential to continued critical infrastructure viability, including staffing operations centers, maintaining and repairing critical infrastructure, operating call centers, working construction, and performing management functions, among others." CISA added that "[t]he

industries they support represent, but are not necessarily limited to, medical and healthcare, telecommunications, information technology systems, defense, food and agriculture, transportation and logistics, energy, water and wastewater, law enforcement, and public works."

However, the key point here is that state and local governments will be left to ultimately make this designation as CISA either lacks the authority or is declining to exercise that authority right now consistent with many other aspects of the Trump Administration's response to COVID-19. Consequently, these governments may ultimately not agree with the claim that ABA workers are clearly essential.

In the attached cover letter to the memo, CISA Director Christopher Krebs explained

> **...this list is advisory in nature. It is not, nor should it be considered to be, a federal directive or standard in and of itself (emphasis in the original)**

Krebs added that "[w]e recognize that State, local, tribal, and territorial governments are ultimately in charge of implementing and executing response activities in communities under their jurisdiction, while the Federal government is in a supporting role." He continued, "[a]s State and local governments consider COVID-19-related restrictions, CISA is offering this list to assist prioritizing activities related to continuity of operations and incident response, including the appropriate movement of critical infrastructure workers within and between jurisdictions."

CISA listed the "THE IMPORTANCE OF ESSENTIAL CRITICAL INFRASTRUCTURE WORKERS:

- Functioning critical infrastructure is imperative during the response to the COVID-19 emergency for both public health and safety as well as community well-being. Certain critical infrastructure industries have a special responsibility in these times to continue operations.
- This guidance and accompanying list are intended to support State, Local, and industry partners in identifying the critical infrastructure sectors and the essential workers needed to maintain the services and functions Americans depend on daily and that need to be able to operate resiliently during the COVID-19 pandemic response.
- This document gives guidance to State, local, tribal, and territorial jurisdictions and the private sector on defining essential critical infrastructure workers. Promoting the ability of such workers to continue to work during periods of community restriction, access management, social distancing, or closure orders/directives is crucial to community resilience and continuity of essential functions.

CISA enumerated "CONSIDERATIONS FOR GOVERNMENT AND BUSINESS," a "list was developed in consultation with federal agency partners, industry experts, and State and local officials, and is based on several key principles:

1. Response efforts to the COVID-19 pandemic are locally executed, State managed, and federally supported
2. Everyone should follow guidance from the CDC, as well as State and local government officials, regarding strategies to limit disease spread.
3. Workers should be encouraged to work remotely when possible and focus on core business activities. In- person, non-mandatory activities should be delayed until the resumption of normal operations.
4. When continuous remote work is not possible, businesses should enlist strategies to reduce the likelihood of spreading the disease. This includes, but is not necessarily limited to,

separating staff by off-setting shift hours or days and/or social distancing. These steps can preserve the workforce and allow operations to continue.
5. All organizations should implement their business continuity and pandemic plans, or put plans in place if they do not exist. Delaying implementation is not advised and puts at risk the viability of the business and the health and safety of the employees.
6. In the modern economy, reliance on technology and just-in-time supply chains means that certain workers must be able to access certain sites, facilities, and assets to ensure continuity of functions.
7. Government employees, such as emergency managers, and the business community need to establish and maintain lines of communication.
8. When government and businesses engage in discussions about critical infrastructure workers, they need to consider the implications of business operations beyond the jurisdiction where the asset or facility is located. Businesses can have sizeable economic and societal impacts as well as supply chain dependencies that are geographically distributed.
9. Whenever possible, jurisdictions should align access and movement control policies related to critical infrastructure workers to lower the burden of workers crossing jurisdictional boundaries.

NIST has re-released its "guidelines on telework and remote access to help organizations mitigate security risks associated with the enterprise technologies used for teleworking, such as remote access servers, telework client devices, and remote access communications." NIST noted that "Special Publication (SP) 800-46 Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security" was issued in 2016, and its recommendations are still relevant today." NIST's "Information Technology Laboratory (ITL) Bulletin summarizes key concepts and recommendations from SP 800-46 Revision 2, [which] include deploying some or all of the following security measures:

- Developing and enforcing a telework security policy, such as having tiered levels of remote access
- Requiring multi-factor authentication for enterprise access
- Using validated encryption technologies to protect communications and data stored on the client devices
- Ensuring that remote access servers are secured effectively and kept fully patched
- Securing all types of telework client devices—including desktop and laptop computers, smartphones, and tablets—against common threats

EDPB Advises EU Governments and Private Sector Entities On Processing Data To Fight COVID-19

In response to calls for the use of location data on smartphones and other data as a means of tracking and combatting the spread of COVID-19, the European Data Protection Board (EDPB) issued a statement explaining its view on how and when that is permissible and legal under European Union (EU) laws and regulations such as the General Data Protection Regulation (GDPR) and the ePrivacy Directive. Given that the EDPB consists of the EU's data protection authorities, the EDPB's statement could inform the regulatory approach they may take regarding how public and private sector entities use data in efforts to address COVID-19.

The EDPB stated that "[g]overnments, public and private organisations throughout Europe are taking measures to contain and mitigate COVID-19…[and] [t]his can involve the processing of different types of personal data." The EDPB stated that "[d]ata protection rules (such as the GDPR) do not

hinder measures taken in the fight against the coronavirus pandemic…[and] [t]he fight against communicable diseases is a valuable goal shared by all nations and therefore, should be supported in the best possible way." The EDPB stated that "[i]t is in the interest of humanity to curb the spread of diseases and to use modern techniques in the fight against scourges affecting great parts of the world." The EDPB wanted "to underline that, even in these exceptional times, the data controller and processor must ensure the protection of the personal data of the data subjects…[and] [t]herefore, a number of considerations should be taken into account to guarantee the lawful processing of personal data and in all cases it should be recalled that any measure taken in this context must respect the general principles of law and must not be irreversible." The EDPB stressed that "[e]mergency is a legal condition which may legitimise restrictions of freedoms provided these restrictions are proportionate and limited to the emergency period."

The EDPB stated that consent from EU persons is not necessary during an epidemic:

> The GDPR is a broad piece of legislation and provides for rules that also apply to the processing of personal data in a context such as the one relating to COVID-19. The GDPR allows competent public health authorities and employers to process personal data in the context of an epidemic, in accordance with national law and within the conditions set therein. For example, when processing is necessary for reasons of substantial public interest in the area of public health. Under those circumstances, there is no need to rely on consent of individuals.

However, the EDPB's stance of using location data is less unequivocal:

> With regard to the processing of telecom data, such as location data, national laws implementing the ePrivacy Directive must also be respected. In principle, location data can only be used by the operator when made anonymous or with the consent of individuals. However, Art. 15 of the ePrivacy Directive enables Member States to introduce legislative measures to safeguard public security. Such exceptional legislation is only possible if it constitutes a necessary, appropriate and proportionate measure within a democratic society. These measures must be in accordance with the Charter of Fundamental Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Moreover, it is subject to the judicial control of the European Court of Justice and the European Court of Human Rights. In case of an emergency situation, it should also be strictly limited to the duration of the emergency at hand.

While not outright barring the collection and processing of the personal data related to EU person's phones, the EDPB suggests workarounds and exceptions that will keep EU governments on legal ground:

> Can Member State governments use personal data related to individuals' mobile phones in their efforts to monitor, contain or mitigate the spread of COVID-19?
>
> In some Member States, governments envisage using mobile location data as a possible way to monitor, contain or mitigate the spread of COVID-19. This would imply, for instance, the possibility to geolocate individuals or to send public health messages to individuals in a specific area by phone or text message. Public authorities should first seek to process location data in an anonymous way (ie. processing data aggregated in a way that

> individuals cannot be re-identified), which could enable generating reports on the concentration of mobile devices at a certain location ("cartography").

The EDPB also reminded controllers that "[p]ersonal data protection rules do not apply to data which has been appropriately anonymised." But, the EDPB also referenced the ePrivacy Directive's exception, which hinges on the enactment of legislation in each country:

> When it is not possible to only process anonymous data, the ePrivacy Directive enables Member States to introduce legislative measures to safeguard public security (Art. 15).
> If measures allowing for the processing of non-anonymised location data are introduced, a Member State is obliged to put in place adequate safeguards, such as providing individuals of electronic communication services the right to a judicial remedy.

Finally, the EDPB cautioned that "[t]he proportionality principle also applies…[and] [t]he least intrusive solutions should always be preferred, taking into account the specific purpose to be achieved." The EDPB stated

> Invasive measures, such as the "tracking" of individuals (i.e. processing of historical non-anonymised location data) could be considered proportional under exceptional circumstances and depending on the concrete modalities of the processing. However, it should be subject to enhanced scrutiny and safeguards to ensure the respect of data protection principles (proportionality of the measure in terms of duration and scope, limited data retention and purpose limitation).

The GDPR contains language allowing for EU nations to act without consent in terms of collecting and processing personal data. For example, in the GDPR's findings section, it is asserted that "[s]ome types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters." Section 9 of the GDPR details the general bar to data processing that reveals a range of sensitive information such as "data for the purpose of uniquely identifying a natural person, data concerning health…" However, one of the enumerated exceptions allow for data processing under these circumstances is for

> processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

NIST Releases Final Draft of Major Guidance Document

The National Institute of Standards and Technology (NIST) has released its final draft version of one of its major guidance documents on information security, risk management, privacy, and other related matters. Comments are due by May 15, 2020 on Special Publication (SP) 800-53, Revision 5 "Security and Privacy Controls for Information Systems and Organizations."

NIST explained that

> This catalog of security and privacy controls provides protective measures for systems, organizations, and individuals. The controls are designed to facilitate compliance with applicable laws, executive orders, directives, regulations, policies, and standards. The security and privacy controls in the catalog, with few exceptions, are policy, technology, and sector neutral—meaning the controls focus on the fundamental measures necessary to protect information and the privacy of individuals across the information life cycle. While security and privacy controls are largely policy, technology, and sector neutral, that does not imply that the controls are policy, technology, and sector unaware. Understanding policies, technologies, and sectors is necessary so that the controls are relevant when implemented. Employing a policy, technology, and sector neutral control catalog has many benefits. It encourages organizations to:
>
> - Focus on the security and privacy functions and capabilities required for mission and business success and the protection of information and the privacy of individuals, irrespective of the technologies that are employed in organizational systems;
> - Analyze each security and privacy control for its applicability to specific technologies, environments of operation, missions and business functions, and communities of interest; and
> - Specify security and privacy policies as part of the tailoring process for controls that have variable parameters.

NIST asserted that

> There is an urgent need to strengthen the underlying information systems, component products, and services that we depend on in every sector of the critical infrastructure to help ensure those systems, components, and services are sufficiently trustworthy and provide the necessary resilience to support the economic and national security interests of the United States. This update to NIST Special Publication 800-53 responds to the call by the Defense Science Board by embarking on a proactive and systemic approach to develop comprehensive safeguarding measures for all types of computing platforms, including general purpose computing systems, cyber-physical systems, cloud and mobile systems, industrial/process control systems, and Internet of Things (IoT) devices. Those safeguarding measures include security and privacy controls to protect the critical and essential mission and business operations of organizations, the organization's high value assets, and the personal privacy of individuals. The objective is to make the information systems we depend on more penetration resistant to cyber-attacks; limit the damage from those attacks when they occur; make the systems cyber resilient and survivable; and protect the security and privacy of information.

In a summary, NIST noted "[t]he significant changes to the publication (from Revision 4) include:

- Creating security and privacy controls that are more outcome-based by changing the structure of the controls. The technical content of the control remains unchanged as a result of making the control statement more outcome-focused. Using AC-3, Access Enforcement, as an example:
  - NIST SP 800-53, Revision 4, AC-3:
    - The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
  - NIST SP 800-53, Revision 5, AC-3:

        - Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
    - Appendix D, Control Summaries in Revision 5, indicates if a control or control enhancement is typically implemented by an information system through technical means with an "S" in the implemented by column. A control or control enhancement that is typically implemented by an organization (i.e., by an individual through nontechnical means) is indicated by an "O" in the implemented by column. A control or control enhancement that can be implemented by an organization or a system or a combination of the two, is indicated by an "O/S".
- Adding two new control families for privacy and supply chain risk management. The Personally Identifiable Information Processing and Transparency family addresses privacy risk management and the Supply Chain Risk Management family leverages and expands on technical concepts from the Revision 4 control, SA-12, Supply Chain Protection.
- Fully integrating privacy controls into the security control catalog, creating a consolidated and unified set of controls. NIST SP 800-53, Revision 4 added an appendix of privacy controls and related implementation guidance (Appendix J) based on the Fair Information Practice Principles. Revision 5 continues the incorporation of privacy into the control catalog by expanding the suite of privacy controls and moving them from an appendix into the fully integrated main catalog through integration with relevant security controls and a new family, Personally Identifiable Information Processing and Transparency. The expanded control catalog also includes specific references to OMB's guidance on breach response and the Foundations for Evidence-Based Policymaking Act of 2018.
- Integrating the Program Management control family into the consolidated catalog of controls. To facilitate ease of use and uniform presentation of control families, the Program Management (PM) family of controls was incorporated into the main control catalog.
- Separating the control selection process from the controls—allowing controls to be used by different communities of interest. Different organizations may elect to use different processes to select applicable controls. Revision 5 no longer includes selection guidance for the controls; that guidance can be found NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.
- Separating the control catalog from the control baselines. To further support the use of Revision 5 by different communities of interest, the control baselines have been moved to NIST SP 800-53B, Control Baselines and Tailoring Guidance for Federal Information Systems and Organizations, projected for publication in 2020. SP 800-53B also provides guidance for tailoring control baselines and for developing overlays to support security and privacy requirements of stakeholders and their organizations.
- Promoting alignment with different risk management and cybersecurity approaches and lexicons, including the NIST Cybersecurity and Privacy Frameworks. By separating the control selection process from the controls, the controls can be used to support other cybersecurity lexicons and risk management approaches.
- Clarifying the relationship between security and privacy to improve the selection of controls necessary to address the full scope of security and privacy risks. A new section in Chapter Two, Security and Privacy Controls has been added.
- Incorporating new, state-of-the-practice controls based on threat intelligence, empirical attack data, and systems engineering and supply chain risk management best practices. New controls in Revision 5:
    - Strengthen security and privacy governance and accountability;
    - Support secure system design; and

    - Support cyber resiliency and system survivability.
- Supplemental Resources will be made available online pending final publication of SP 800-53, Revision 5. Examples of supplemental resources include:
    - Mappings to ISO 27001 and ISO 15408;
    - Mappings to the NIST Cybersecurity and Privacy Frameworks;
    - Control and control enhancement keywords; and
    - SP 800-53 controls in machine-readable format (using Open Security Controls Assessment Language [OSCAL]).

Members Urge President and Vice President To Set Up Privacy Limits For Data Used In COVID-19 Response

Representatives Suzan DelBene (D-WA) and Anna Eshoo (D-CA) and Senator Ron Wyden (D-OR) sent a letter to President Donald Trump and Vice President Vice President Mike Pence outlining the privacy principles that they believe should guide the Administration's "work with technology companies and other private sector actors in coordinating our country's responses to the COVID-19 pandemic." Presumably, these principles could be written into contracts or agreements with private sector entities and the Administration could also direct federal agencies to operate from these precepts, but it is unlikely the Administration will agree to do so.

DelBene, Eshoo, and Wyden explained "[w]e support bold measures to keep Americans safe and healthy during this crisis. However, prohibiting government intrusion into the private lives of Americans is, and has always been part of the DNA of our country, enshrined in the Fourth Amendment of our Constitution." They stated that "[b]ecause location and health data are some of the most private types of information about any individual, we urge you to implement procedures to protect the privacy of Americans by adopting the following privacy principles:

1) Aggregation, Minimization, and Anonymization. The federal government should only collect data that may be directly useful in responding to the current public health crisis. If appropriate for anticipated uses, the government should limit collection to aggregated data and trends from companies. If aggregated information is insufficient, minimize data to what public health experts identify as necessary. Where practicable, anonymize datasets by removing associated data and meta data unnecessary for the specifically intended public health uses.

2) Use Limitations

a. Private Company Uses. The Administration should require that private companies collecting data specific to the COVID-19 crisis, such as information about individuals who are searching for testing centers or information about the disease, must not be able to use such data for any other purpose. The data must not, for example, be combined with behavioral targeting data or be used to train machine learning algorithms to improve advertising.

b. Governmental Uses. Prohibit any government agency or employee from disclosing, transferring, or selling information to agencies, companies or other organizations, or individuals not directly involved with the public health response to COVID-19. Under no circumstances should this data be shared with law enforcement or immigration agencies.

3) Data Security. Data should be transferred and stored using the highest cybersecurity protocols.

4) Prohibiting Reidentification. Prohibit attempts to reidentify specific individuals from aggregate or anonymized datasets.

5) Destruction of Data After Pandemic. Upon conclusion of the pandemic, require all government agencies, employees, and contractors to delete identifiable data. Retaining data beyond the specific crisis creates additional privacy concerns.

Since this letter was sent, a number of federal agencies have signaled an intention to ease up on some privacy requirements so that regulated entities can better address the effects of COVID-19.

The Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) announced last week that "effective immediately,…it will exercise its enforcement discretion and will waive potential penalties for HIPAA violations against health care providers that serve patients through everyday communications technologies during the COVID-19 nationwide public health emergency." OCR "is responsible for enforcing certain regulations issued under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act, to protect the privacy and security of protected health information, namely the HIPAA Privacy, Security and Breach Notification Rules (the HIPAA Rules)" as explained in a "Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency." OCR stated it "will exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA Rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency."

OCR explained

- Under this Notice, covered health care providers may use popular applications that allow for video chats, including Apple FaceTime, Facebook Messenger video chat, Google Hangouts video, Zoom, or Skype, to provide telehealth without risk that OCR might seek to impose a penalty for noncompliance with the HIPAA Rules related to the good faith provision of telehealth during the COVID-19 nationwide public health emergency.
- Providers are encouraged to notify patients that these third-party applications potentially introduce privacy risks, and providers should enable all available encryption and privacy modes when using such applications.
- Under this Notice, however, Facebook Live, Twitch, TikTok, and similar video communication applications are public facing, and should not be used in the provision of telehealth by covered health care providers.

OCR added

Covered health care providers that seek additional privacy protections for telehealth while using video communication products should provide such services through technology vendors that are HIPAA compliant and will enter into HIPAA business associate agreements (BAAs) in connection with the provision of their video communication products. The list below includes some vendors that represent that they provide HIPAA-compliant video communication products and that they will enter into a HIPAA BAA.

- Skype for Business / Microsoft Teams
- Updox
- VSee
- Zoom / Zoom for Healthcare
- Doxy.me
- Google G Suite Hangouts Meet

- Cisco Webex Meetings / Webex Teams
- Amazon Chime
- GoToMeeting

DOD OIG Finds A Lack of Progress Eight Years After Previous Audit of DOD Cyber Red Teams

The Department of Defense's Office of the Inspector General (OIG) has released a follow up audit of the Department of Defense's (DOD) Cyber Red Teams to determine whether the problems turned up in the earlier audit were addressed. The short answer is these problems were largely not addressed in effective fashion, and so the DOD OIG is again calling on the DOD, especially the National Security Agency (NSA), to effectively identify problems turned up during the penetrations carried out by the DOD's Cyber Red Teams and for the DOD component agencies to remedy those vulnerabilities the Red Teams exploit and use. This audit goes to larger issues at the Pentagon regarding its cyber defenses.

The OIG stated that

> The objective of this followup audit was to determine whether DOD Cyber Red Teams and DOD Components took actions to correct problems identified in Report No. DODIG-2013-035, "Better Reporting and Certification Processes Can Improve Red Teams' Effectiveness," December 21, 2012. In addition, we determined whether DOD Cyber Red Teams supported operational testing and combatant command exercises to identify network vulnerabilities, threats, and other security weaknesses affecting DOD systems, networks, and facilities, and whether corrective actions were taken to address DOD Cyber Red Team findings. We also assessed risks affecting the ability of DOD Cyber Red Teams to support DOD missions and priorities.

The OIG explained that "[t]he DOD uses DOD Cyber Red Teams to highlight vulnerabilities, improve joint cyberspace operations, and protect the DOD Information Network and DOD weapons systems from vulnerabilities and threats that affect the DOD's security posture." However, Red Teams do not use traditional vulnerabilities and instead "use known vulnerabilities, zero day attacks (attacks that exploit a previously unknown hardware, firmware, or software vulnerability), and other tactics an adversary may use to penetrate systems, networks, and facilities, and test the defense-in-depth strength (use of multiple barriers and layers of defenses and responses taken to DOD Cyber Red Team actions). As of last fall, there are ten accredited Red Teams at the NSA.

The OIG "determined that the DOD Components did not consistently mitigate or include unmitigated vulnerabilities identified in the prior audit and during this audit by DOD Cyber Red Teams during combatant command exercises, operational testing assessments, and agency-specific testing in plans of action and milestones." Moreover, the OIG stated "[t]he DOD Components did not consistently mitigate vulnerabilities or include unmitigated vulnerabilities in plans of action and milestones because they failed to assess the impact of the vulnerabilities to their mission, prioritize resources to implement risk mitigation solutions, or coordinate the results of DOD Cyber Red Teams reports with applicable stakeholders.: The OIG added "the DOD did not have an organization responsible for ensuring that DOD Components took action to manage vulnerabilities identified by DOD Cyber Red Teams and did not establish processes that held DOD Components responsible for mitigating those vulnerabilities."

The OIG also "determined that the DOD did not establish a unified approach to support and

prioritize DOD Cyber Red Team missions...[and] the DOD Components implemented Component-specific approaches to staff, train, and develop tools for DOD Cyber Red Teams, and prioritize DOD Cyber Red Team missions." The OIG stated that "[t]he DOD did not

- assign an organization with responsibility to oversee and synchronize DOD Cyber Red Team activities based on DOD needs and priorities;
- assess the resources needed for each DOD Cyber Red Team and identify core requirements to staff and train them to meet DOD priorities; or
- develop baseline tools to perform assessments

The OIG recommended that the Secretary of Defense assign an organization with responsibility to, among other actions:

- review and assess DOD Cyber Red Team reports for systemic vulnerabilities and coordinate the development and implementation of enterprise solutions to mitigate those vulnerabilities;
- ensure DOD Components develop and implement a risk-based process to assess the impact of DOD Cyber Red Team-identified vulnerabilities and prioritize funding for corrective actions for high-risk vulnerabilities;
- ensure DOD Components develop and implement processes for providing reports with DOD Cyber Red Team findings and recommendations to organizations with responsibility for corrective actions;
- develop processes and procedures to oversee DOD Cyber Red Team activities, including synchronizing and prioritizing DOD Cyber Red Team missions, to ensure these activities align with DOD priorities;
- perform a joint DOD-wide mission-impact analysis to determine the number of DOD Cyber Red Teams, minimum staffing levels of each team, the composition of the staffing levels needed to meet current and future DOD Cyber Red Team mission requests;
- assess and identify a baseline of core and specialized training standards, based on the three DOD Cyber Red Team roles that DOD Cyber Red Team staff must meet for the team to be certified and accredited; and
- identify and develop baseline tools needed by DOD Cyber Red Teams to perform missions

The OIG also recommended that

- the Chairman of the Joint Chiefs of Staff revise Chairman of the Joint Chiefs of Staff Instruction 6510.05 and Chairman of the Joint Chiefs of Staff Manual 6510.02 to include requirements for addressing DOD Cyber Red Team-identified vulnerabilities and reporting actions taken to mitigate those vulnerabilities.
- the Commanders for U.S. Strategic Command and U.S. Southern Command, Program Manager Advance Amphibious Assault for the Amphibious Combat Vehicle; and Director for the Defense Forensics and Biometric Agency assess and prioritize the risk of each unmitigated vulnerability identified in the Red Team assessments, take immediate actions to mitigate high-risk vulnerabilities, and if unable to immediately mitigate the vulnerabilities, include them on a command- approved plan of action and milestones.

NIST Illustrates Examples of How Agencies Can Use Cybersecurity Framework

The National Institute of Standards and Technology (NIST) has released a guidance document with example approaches of how federal agencies could use the Framework for Improving Critical Infrastructure Cybersecurity (aka Cybersecurity Framework) to improve cybersecurity generally and to help meet and/or complement efforts to meet binding federal requirements. The guidance document is meant to be informative and is intended for those with the responsibility to manage

information systems at federal agencies, especially "personnel who develop, implement, report, and improve enterprise and cybersecurity risk management processes within their organizations." NIST added "that many public and private sector organizations that choose to use the NIST cybersecurity risk management suite of standards and guidelines will benefit from this document."

Of course, the May 2017 Executive Order, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," directs each agency to "use [the Cybersecurity Framework] developed by [NIST], or any successor document, to manage the agency's cybersecurity risk." This mandate thus lends this guidance document more importance than some of NIST's other guidance, for an agency may employ these approaches under the cover of NIST's imprimatur, and the Office of Management and Budget (OMB) may be more willing to accept appropriate usage of these approaches. Additionally, a number of the examples eplicitly refer to other NIST Special Publications (e.g. SP 800-39, Managing Information Security Risk), which will likely result in these publications becoming more widely adhered to. Moreover, if agencies more widely implement the Cybersecurity Framework and the supporting documents, it is likely this will have a flow down effect on entities contracting with the federal government.

NIST stated that National Institute of Standards and Technology Interagency or Internal Report 8170, "Approaches for Federal Agencies to Use the Cybersecurity Framework," provides "examples for implementing the Cybersecurity Framework in a manner that complements the use of other NIST security and privacy risk management standards, guidelines, and practices." NIST added that "[t]hese examples include support for an Enterprise Risk Management (ERM) approach in alignment with OMB and Federal Information Security Management Act (FISMA) requirements that agency heads "manage risk commensurate with the magnitude of harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of a federal information system or federal information."

NIST stated that

> Using eight example approaches, this section provides guidance to assist federal agencies as they develop, implement, and continuously improve their cybersecurity risk management programs. The examples are consistent with OMB Circular A-130, Managing Information as a Strategic Resource, which provides guidance regarding the heavily used NIST Risk Management Framework, associated documents, and the Cybersecurity Framework. The examples also support OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Control; use of the Cybersecurity Framework helps to identify, manage, report, and monitor the internal controls needed to properly manage potential information and technology risks to an agency.
> All federal agencies are entrusted with safeguarding the information contained in their systems and ensuring that those systems operate securely and reliably. It is vital that agency personnel at all levels manage their assets wisely and address cybersecurity risks effectively. To do that, agencies need a holistic approach to their enterprises' risk management that includes timely, streamlined approaches and automated tools.

NIST asserted that

> As part of its statutory responsibilities under the Federal Information Security Management Act as amended (FISMA), the National Institute of Standards and Technology (NIST) develops standards and guidelines—including minimum requirements—to provide

> adequate information security for federal information and information systems. This suite of security and privacy risk management standards and guidelines provides guidance for an integrated, organization- wide program to manage information security risk. NIST produced this report to assist federal agencies in strengthening their cybersecurity risk management processes by highlighting example approaches for implementing the Framework for Improving Critical Infrastructure Cybersecurity (known as the Cybersecurity Framework). Developed by NIST in close collaboration with private and public sectors, the Cybersecurity Framework is a risk-based approach used voluntarily by organizations across the United States. Initially developed to address cybersecurity challenges in the Nation's Critical Infrastructure (CI) sectors, the voluntary Framework is used by a variety of organizations across the world. The Cybersecurity Framework aligns with and complements NIST's suite of security and privacy risk management standards and guidelines.

NIST stated that "[t]his report illustrates eight example approaches through which federal agencies can leverage the Cybersecurity Framework to address common cybersecurity-related responsibilities...[and] [b]y doing so, agencies can integrate the Cybersecurity Framework with key NIST cybersecurity risk management standards and guidelines that are already in wide use." NIST stated that "[t]hese eight approaches support a mature agency-wide cybersecurity risk management program:

1. Integrate enterprise and cybersecurity risk management
2. Manage cybersecurity requirements
3. Integrate and align cybersecurity and acquisition processes
4. Evaluate organizational cybersecurity
5. Manage the cybersecurity program
6. Maintain a comprehensive understanding of cybersecurity risk
7. Report cybersecurity risks
8. Inform the tailoring process

HHS Releases EHR Final Rules

Two agencies of the Department of Health and Human Services (HHS) released two long awaited final rules that could change how electronic health records (EHR) are employed. In its press release, HHS claimed that "[i]nteroperability has been pursued by multiple administrations and numerous laws, and today, these rules finally deliver on giving patients true access to their healthcare data to make informed healthcare decisions and better manage their care. Putting patients in charge of their health records is a key piece of giving patients more control in healthcare, and patient control is at the center of the Trump administration's work toward a value-based healthcare system.

HHS stated that "[t]he two rules, issued by the HHS Office of the National Coordinator for Health Information Technology (ONC) and Centers for Medicare & Medicaid Services (CMS), implement interoperability and patient access provisions of the bipartisan 21st Century Cures Act (Cures Act) and support President Trump's MyHealthEData initiative…[which] is designed to empower patients around a common aim - giving every American access to their medical information so they can make better healthcare decisions." HHS stated that "[t]ogether, these final rules mark the most extensive healthcare data sharing policies the federal government has implemented, requiring both public and private entities to share health information between patients and other parties while keeping that information private and secure, a top priority for the Administration."

HHS explained the two rules:

- **Addressing Interoperability and Information Blocking**
  - The ONC Final Rule identifies and finalizes the reasonable and necessary activities that do not constitute information blocking while establishing new rules to prevent "information blocking" practices (e.g., anti-competitive behaviors) by healthcare providers, developers of certified health IT, health information exchanges, and health information networks as required by the Cures Act.
  - Currently, many EHR contracts contain provisions that either prevent or are perceived to prevent users from sharing information related to the EHRs in use, such as screen shots or video. The ONC final rule updates certification requirements for health IT developers and establishes new provisions to ensure that providers using certified health IT have the ability to communicate about health IT usability, user experience, interoperability, and security including (with limitations) screenshots and video, which are critical forms of visual communication for such issues.
  - The ONC final rule also requires electronic health records to provide the clinical data necessary, including core data classes and elements, to promote new business models of care. This rule advances common data through the U.S. Core Data for Interoperability (USCDI). The USCDI is a standardized set of health data classes and data elements that are essential for nationwide, interoperable health information exchange. The USCDI includes "clinical notes," allergies, and medications among other important clinical data, to help improve the flow of electronic health information and ensure that the information can be effectively understood when it is received. It also includes essential demographic data to support patient matching across care settings.
- **Unleashing Innovation & Patient Access**
  - ONC's final rule establishes secure, standards-based application programming interface (API) requirements to support a patient's access and control of their electronic health information. APIs are the foundation of smartphone applications (apps). As a result of this rule, patients will be able to securely and easily obtain and use their electronic health information from their provider's medical record for free, using the smartphone app of their choice.
  - Building on the foundation established by ONC's final rule, the CMS Interoperability and Patient Access final rule requires health plans in Medicare Advantage, Medicaid, CHIP, and through the federal Exchanges to share claims data electronically with patients. CMS took the first step towards interoperability by launching Medicare Blue Button 2.0 for Medicare beneficiaries in 2018. Medicare Blue Button 2.0 gives beneficiaries the ability to securely connect their Medicare Part A, Part B and Part D claims and encounter data to apps and other tools developed by innovators. Engagement and partnership with the technology community has involved more than 2,770 developers from over 1,100 organizations working in the Medicare Blue Button 2.0 sandbox to develop innovative apps to benefit Medicare patients. Currently, 55 organizations have applications in production. Beginning January 1, 2021, Medicare Advantage, Medicaid, CHIP, and, for plan years beginning on or after January 1, 2021, plans on the federal Exchanges will be required to share claims and other health information with patients in a safe, secure, understandable, user-friendly electronic format through the Patient Access API. With more complete data in their hands, patients can be more informed decision makers leading to better informed treatment.
  - This Patient Access API will allow patients to access their data through any third party application they choose to connect to the API and could also be used to

integrate a health plan's information to a patient's electronic health record (EHR). By requiring their relevant health information including their claims to be shared with them, patients can take this information with them as they move from plan to plan, and provider to provider throughout the healthcare system.

- To further advance the mission of fostering innovation, the CMS final rule establishes a new Condition of Participation (CoP) for all Medicare and Medicaid participating hospitals, requiring them to send electronic notifications to another healthcare facility or community provider or practitioner when a patient is admitted, discharged, or transferred. These notifications can facilitate better care coordination and improve patient outcomes by allowing a receiving provider, facility, or practitioner to reach out to the patient and deliver appropriate follow-up care in a timely manner. Additionally, CMS is requiring states to send enrollee data daily beginning April 1, 2022 for beneficiaries enrolled in both Medicare and Medicaid, improving the coordination of care for this population. This ensures beneficiaries are getting access to appropriate services and that these services are billed appropriately the first time, eliminating waste and burden. Beneficiaries will get the right services at the right time at the right cost, with no administrative burden to rebill services.

Further Reading

- "Hackers had access to European electricity organization's email server for weeks: report" – *cyberscoop*
- "High-Stakes Security Setups Are Making Remote Work Impossible" – *WIRED*
- "Federal employees may soon be ordered to work from home. That could pose serious cybersecurity risks" – *The Washington Post*
- "Israel deploys cyber-monitoring against coronavirus, tells people not to leave home" – *Reuters*
- "U.S. government, tech industry discussing ways to use smartphone location data to combat coronavirus" – *The Washington Post*
- "Israeli Spyware Firm Wants to Track Data to Stop Coronavirus Spreading" – *Bloomberg*
- "Facebook's misinformation problem goes deeper than you think" – *The Verge*
- "Russian hackers using stolen corporate email accounts to mask their phishing attempts" – *cyberscoop*
- "The Coder and the Dictator" – *The New York Times*
- "Working from home can make people more productive. Just not during a pandemic." – *Recode*
- "Coronavirus Is Speeding Up the Amazonification of the Planet" – *OneZero*