Akin Gump
STRAUSS HAUER & FELD LLP

Agency Deadlines Under Cybersecurity Information Sharing Act of 2015 (H.R. 2029, Division N, Title I)			
Section	**Agency**	**Regulatory Requirement**	**Deadline**
103(a)(1), Sharing of Information by the Federal Government	DNI, DHS, DOD, DOJ	"shall jointly develop and issue procedures to facilitate and promote the timely sharing of classified cyber threat indicators and defensive measures in the possession of the Federal Government with representatives of relevant Federal entities and non-Federal entities that have appropriate security clearances"	DNI must submit procedures to Congress within 60 days of enactment
105, Sharing of Cyber Threat Indicators and Defensive Measures with the Federal Government	DOJ and DHS	Must jointly develop interim and final policies "relating to the receipt of cyber threat indicators and defensive measures by the Federal Government"	Interim policies must be submitted to Congress within 60 days; final policies within 180 days
105(a)(4), Guidelines for Entities Sharing Cyber Threat Indicators with the Federal Government	DOJ and DHS	"shall jointly develop and make publicly available guidance to assist entities and promote sharing of cyber threat indicators with Federal entities"	Must jointly submit guidance within 60 days of enactment
105(b), Privacy and Civil Liberties	DOJ and DHS	"shall jointly develop, submit to Congress, and make available to the public interim guidelines relating to privacy and civil liberties which shall govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity"	Interim guidelines must be submitted to Congress within 60 days; final guidelines within 180 days
105(c), Capability and Process within the DHS	DHS	DHS "shall develop and implement a capability and process within the Department of Homeland Security that receives cyber threat indicators and defensive measures under this title that are shared by a non-Federal entity with the Federal Government and ensures that all of the appropriate Federal entities receive in an automated manner such cyber threat indicators and defensive measures shared through the real-time process"	Within 90 days of enactment (DHS must submit a certification of capability to Congress within same time period)
107(a)(1), Oversight of Government Activities	"heads of the appropriate Federal entities"	"shall jointly submit to Congress a detailed report concerning the implementation of this title"	Within one year of enactment
107(b), Biennial Report on Compliance	Inspectors General of appropriate Federal entities	"shall jointly submit to Congress an interagency report on the actions of the executive branch of the Federal Government to carry out this title during the most recent 2-year period"	Not later than two years after the date of enactment of this Act and not less frequently than once every two years thereafter
107(c), Independent Report on Removal of Personal Information	U.S. Comptroller General	"shall submit to Congress a report on the actions taken by the Federal Government to remove personal information from cyber threat indicators or defensive measures pursuant to this title"	Not later than three years after the date of enactment

109, Report on Cybersecurity Threats	DNI	"shall submit to the Select Committee on Intelligence of the Senate and the Permanent Select Committee on Intelligence of the House of Representatives a report on cybersecurity threats, including cyber attacks, theft, and data breaches"	Not later than 180 days after the date of enactment
111, Effective Period	N/A	"this title and the amendments made by this title shall be effective during the period beginning on the date of the enactment of this Act and ending on September 30, 2025"	Law sunsets within 10 years
National Cybersecurity Advancement Act (Division N, Title II)			
Section	**Agency**	**Regulatory Requirement**	**Deadline**
203(5)"(g)," Automated Information Sharing	DHS	"in coordination with industry and other stakeholders, shall develop capabilities making use of existing information technology industry standards and best practices, as appropriate, that support and rapidly advance the development, adoption, and implementation of automated mechanisms for the sharing of cyber threat indicators and defensive measures in accordance with title I"	DHS must submit annual reports to Congress until implementation is fully complete
203(5)"(j)," Reports on International Cooperation	DHS	"shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report on the range of efforts underway to bolster cybersecurity collaboration with relevant international partners"	Not later than 180 days after the date of enactment
203(5)"(k)," Outreach	DHS	"shall disseminate to the public information about how to voluntarily share cyber threat indicators and defensive measures with the [NCCIC]; and enhance outreach to critical infrastructure owners and operators for purposes of such sharing"	Not later than 60 days after the date of enactment
206, Report on Reducing Cybersecurity Risks in DHS Data Centers	DHS	"shall submit to the appropriate congressional committees a report on the feasibility of the Department creating an environment for the reduction in cybersecurity risks in Department data centers"	Not later than one year after the date of enactment
207, Assessment	U.S. Comptroller General	"shall submit to the appropriate congressional committees a report that includes an assessment of the implementation by [DHS] and the amendments made by this title; and to the extent practicable, findings regarding increases in the sharing of cyber threat indicators, defensive measures, and information relating to cybersecurity risks and incidents at the [NCCIC]"	Not later than two years after the date of enactment
208, Multiple Simultaneous Cyber Incidents at Critical Infrastructure	DHS	"shall provide information to the appropriate congressional committees on the feasibility of producing a risk-informed plan to address the risk of multiple simultaneous cyber incidents affecting critical infrastructure"	Not later than one year after the date of enactment
209, Report on Cybersecurity Vulnerabilities at U.S. Ports	DHS	"shall submit to the appropriate congressional committees, the Committee on Commerce, Science and Transportation of the Senate, and the Committee on Transportation and Infrastructure of the House of Representatives a report on cybersecurity vulnerabilities for the 10 United States ports that the Secretary determines are at greatest risk of a cybersecurity incident and provide recommendations to mitigate such vulnerabilities"	Not later than 180 days after the date of enactment

211, Termination of Reporting Requirements	N/A	"Any reporting requirements in this subtitle shall terminate on the date that is 7 years after the date of enactment of this Act"	Reporting requirements terminate seven years after enactment
223(a)"228(b)(1)," Intrusion Assessment Plan	DHS	"in coordination with the Director of the Office of Management and Budget, [DHS] shall develop and implement an intrusion assessment plan to proactively detect, identify, and remove intruders in agency information systems on a routine basis; and update such plan as necessary"	No deadline
223(a)"230(b)," Intrusion Detection and Prevention System	DHS	"shall deploy, operate, and maintain, to make available for use by any agency, with or without reimbursemen a capability to detect cybersecurity risks in network traffic transiting or traveling to or from an agency information system; and a capability to prevent network traffic associated with such cybersecurity risks from transiting or traveling to or from an agency information system or modify such network traffic to remove the cybersecurity risk"	Not later than one year after the date of enactment
223(a)"230(f)," Privacy Officer Review	DHS Privacy Officer	"Privacy Officer appointed under section 222, in consultation with the Attorney General, shall review the policies and guidelines for the program carried out under this section to ensure that the policies and guidelines are consistent with applicable privacy laws, including those governing the acquisition, interception, retention, use, and disclosure of communications"	Not later than one year after the date of enactment
223(b), Agency Responsibilities	Agency Heads	"the head of each agency shall apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system"	Not later than one year after the date of enactment of this Act or two months after the date on which the Secretary makes available the intrusion detection and prevention capabilities
224, Advanced Internal Defenses	OMB and DHS	"[OMB] shall develop and [DHS] shall implement a plan to ensure that each agency utilizes advanced network security tools to detect and mitigate intrusions and anomalous activity"	No deadline
225(b), Cybersecurity Requirements at Agencies	Heads of Each Agency	"identify sensitive and mission critical data stored by the agency; assess access controls to the data described in subparagraph (A), the need for readily accessible storage of the data, and individuals' need to access the data; encrypt or otherwise render indecipherable to unauthorized users the data that is stored on or transiting agency information systems; and implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication"	Not later than one year after the date of the enactment
226(b), Assessment; Reports - Third-Party Assessment	U.S. Comptroller General	"shall conduct a study and publish a report on the effectiveness of the approach and strategy of the Federal Government to securing agency information systems, including the intrusion detection and prevention capabilities and the intrusion assessment plan"	Not later than three years after the date of enactment
226(c)(1)(A), Assessment; Reports - Reports to Congress	DHS	"shall submit to the appropriate congressional committees a report on the status of implementation of the intrusion detection and prevention capabilities"	Not later than six months after the date of enactment, and annually thereafter

226(c)(1)(B), Assessment; Reports - Reports to Congress	OMB	"shall submit to Congress an analysis of agency application of the intrusion detection and prevention capabilities"	Not later than 18 months after the date of enactment of this Act, and annually thereafter
226(c)(1)(C), Assessment; Reports - Reports to Congress	Federal Chief Information Officer	"shall review and submit to the appropriate congressional committees a report assessing the intrusion detection and intrusion prevention capabilities"	Not earlier than 18 months after the date of enactment and not later than two years after the date of enactment
226(c)(2), Assessment; Reports - Reports to Congress	OMB	"submit the intrusion assessment plan to the appropriate congressional committees"	Not later than six months after the date of enactment of this Act, and 30 days after any update thereto
227, Termination	N/A	"The authority provided under section 230 of the Homeland Security Act of 2002, as added by section 223(a)(6) of this division, and the reporting requirements under section 226(c) of this division shall terminate on the date that is 7 years after the date of enactment of this Act"	Reporting requirements sunset within seven years
228, Identification of Information Systems Relating to National Security	DNI and OMB	"shall identify all unclassified information systems that provide access to information that may provide an adversary with the ability to derive information that would otherwise be considered classified; assess the risks that would result from the breach of each unclassified information system; and assess the cost and impact on the mission carried out by each agency that owns an unclassified information system if the system were to be subsequently designated as a national security system; and (2) DNI and OMB shall submit to the appropriate congressional committees, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives a report that includes the findings"	Not later than 180 days after the date of enactment

Federal Cybersecurity Workforce Assessment (Division N, Title III)			
Section	**Agency**	**Regulatory Requirement**	**Deadline**
303, National Cybersecurity Workforce Measurement Initiative	OPM, NIST	"The head of each Federal agency shall identify all positions within the agency that require the performance of cybersecurity or other cyber-related functions; and assign the corresponding employment code under the National Initiative for Cybersecurity Education"	Not later than 180 days after the date of enactment of this Act, OPM, in coordination with NIST, shall develop a coding structure under the National Initiative for Cybersecurity Education
303, National Cybersecurity Workforce Measurement Initiative	OPM, NIST, DNI	"OPM, in coordination with [DHS, NIST, and DNI], shall establish procedures to implement the National Initiative for Cybersecurity Education coding structure"	Not later than nine months after the date of enactment
303, National Cybersecurity Workforce Measurement Initiative	DOD	"[DOD] shall establish procedures to implement the National Initiative for Cybersecurity Education's coding structure to identify all Federal noncivilian positions that require the performance of information technology, cybersecurity, or other cyberrelated functions"	Not later than 18 months after the date of enactment

303, National Cybersecurity Workforce Measurement Initiative	All Agencies	"The head of each Federal agency shall submit to the appropriate congressional committees of jurisdiction a report that identifies the percentage of personnel with information technology, cybersecurity, or other cyber-related job functions who currently hold the appropriate industry-recognized certifications as identified under the National Initiative for Cybersecurity Education; the level of preparedness of other civilian and noncivilian cyber personnel without existing credentials to take certification exams; and a strategy for mitigating any gaps identified"	Not later than three months after the date on which the procedures are developed
303, National Cybersecurity Workforce Measurement Initiative	All Agencies	"The head of each Federal agency shall establish procedures to identify all encumbered and vacant positions with information technology, cybersecurity, or other cyber-related functions (as defined in the National Initiative for Cybersecurity Education's coding structure); and to assign the appropriate employment code to each such position, using agreed standards and definitions"	Not later than three months after the date on which the procedures are developed
303, National Cybersecurity Workforce Measurement Initiative	All Agencies	"The head of each Federal agency shall complete assignment of the appropriate employment code to each position within the agency with information technology, cybersecurity, or other cyber-related functions"	Not later than one year after the date after the procedures are established
303, National Cybersecurity Workforce Measurement Initiative	OPM	"OPM shall submit a progress report on the implementation of this section to the appropriate congressional committees"	Not later than 180 days after the date of enactment
304, Identification of Cyber-related Work Roles of Critical Need	All Agencies	"The head of each Federal agency, in consultation with [OMB, NIST, and DHS], shall identify information technology, cybersecurity, or other cyber-related work roles of critical need in the agency's workforce; and submit a report to OMB that describes the information technology, cybersecurity, or other cyber-related roles; and substantiates the critical need designations"	Beginning not later than one year after the date on which the employment codes are assigned and annually thereafter
304, Identification of Cyber-related Work Roles of Critical Need	OMB	"[OMB] shall identify critical needs for information technology, cybersecurity, or other cyber-related workforce across all Federal agencies; and submit a progress report on the implementation of this section to the appropriate congressional committees"	Not later than two years after the date of enactment
305, GAO Status Reports	U.S. Comptroller General	"GAO shall submit a report to the appropriate congressional committees that describes the status of such implementation"	Not later than three years after the date of the enactment
Other Cybersecurity Matters (Division N, Title IV)			
Section	**Agency**	**Regulatory Requirement**	**Deadline**
401, Study on Mobile Device Security	DHS, NIST	"[DHS in consultation witn NIST] shall complete a study on threats relating to the security of the mobile devices of the Federal Government; and submit an unclassified report to Congress, with a classified annex if necessary, that contains the findings of such study"	Not later than oneyear after the date of enactment

402, DOS International Cyberspace Policy Strategy	DOS	"Secretary of State shall produce a comprehensive strategy relating to United States international policy with regard to cyberspace"	Not later than 90 days after the date of enactment
404, Enhancement of Emergency Services	DHS	"[DHS] shall establish a process by which a Statewide Interoperability Coordinator may report data on any cybersecurity risk or incident involving any information system or network used by emergency response providers"	Not later than 90 days after the date of enactment
404, Enhancement of Emergency Services	DHS	"[DHS] shall conduct integration and analysis of the data reported under subsection (a) to develop information and recommendations on security and resilience measures for any information system or network used by State emergency response providers"	Not later than one year after the date of enactment
405, Improving Cybersecurity in the Health Care Industry	HHS	"[HHS] shall submit to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and Commerce of the House of Representatives a report on the preparedness of the Department of Health and Human Services and health care industry stakeholders in responding to cybersecurity threats"	Not later than one year after the date of enactment
405, Improving Cybersecurity in the Health Care Industry	HHS	"[HHS] shall convene health care industry stakeholders, cybersecurity experts, and any Federal agencies or entities the [Secretary] determines appropriate to establish a task force to analyze how industries, other than the health care industry, have implemented strategies and safeguards for addressing cybersecurity threats within their respective industries"	Not later than 90 days after the date of enactment. The task force shall terminate on the date that is one year after the date on which such task force is established. Not later than 60 days after the termination of the task force, HHS shall disseminate the information of the task force to health care industry stakeholders in accordance with such paragraph
406, Federal Computer Security	Each federal agency that operates a national security system or a computer system that contains PII	"The Inspector General of each covered agency shall submit to the appropriate committees of jurisdiction in the Senate and the House of Representatives a report regarding the Federal computer systems of the covered agency"	Not later than 240 days after the date of enactment