Sections 4 & 7 4(b): Commerce/NIST identify existing or create standards, tools, and best practices for complying with new software development requirements. 7(c): DHS/CISA provide OMB recommendations on options for implementing a government-wide EDR system.		<ul> <li>Section 3</li> <li>3(b): Agencies share updated plans for adoption and use of cloud technology and implementation plans for zero trust architecture.</li> <li>3(c-iii): DHS/CISA issue a cloud service governance framework for FCEB agencies.</li> <li>3(d-i): Agencies provide progress reports about multifactor authentication and data encryption; new reports are required every 60 days until full adoption is achieved.</li> <li>3(f): GSA/OMB/Agencies start modernizing FedRAMP by establishing training, improving communication, incorporating automation, digitizing and streamlining documentation, and identifying relevant compliance frameworks and mapping them onto requirements.</li> </ul>	Sections 4 & 7 4(h): DHS/CISA/Commerce/NIST identify and make available to agencies a list of software categories and products in use or in the acquisition process that meet the definition of critical software [ref. 4(g)]. 7(f): Agencies establish or update their Memoranda of Agreement (MOA) for the CDM Program to ensure object-level data are available and accessible to CISA.	<ul> <li>Section 3</li> <li>3(c-i): OMB/DHS/CISA/GSA/FedRAMP release a Federal cloud security strategy and guidance for agencies.</li> <li>3(c-ii): DHS/CISA/OMB/GSA/FedRAMP issue cloud security technical reference architecture documentation with recommendations on cloud migration and data protection for FCEB agencies.</li> <li>3(c-iv): Agencies provide reports to DHS/CISA/OMB evaluating types and sensitivity of their unclassified data, including prioritization and appropriate processing and storage.</li> <li>3(e): DHS/CISA/AG/FBI/GSA/FedRAMP establish framework to collaborate on cybersecurity and incident response activities related to FCEB cloud technology.</li> </ul>
JUNE 11	JUNE 26	JULY 11	JULY 26	AUGUST 10
2021	Sections 4 & 7 4(g): Government cybersecurity leaders publish a definition for "critical software" that addresses topics such as level of privilege or	Sections 4 & 7 4(f): Commerce, in coordination with others, publishes minimum elements for a Software Bill of Materials (SBOM). 4(i): Commerce/NIST/DHS/CISA/OMB publish guidance outlining security measures for critical software, covering least		Sections 4 & 7 <b>4(j): OMB</b> takes appropriate steps to require agencies comply with new guidance outlining security measures for critical software [ <i>ref.</i> 4( <i>e</i> )].

## Visit our Executive Order Resource Center at merlincyber.com/EO



## Visit our Executive Order Resource Center at merlincyber.com/EO

**Merlin is the premier cybersecurity platform** with a one-of-a-kind business model that leverages security technologies, trusted relationships, and capital to develop and deliver groundbreaking security solutions that help organizations minimize security risk and simplify IT operations.

