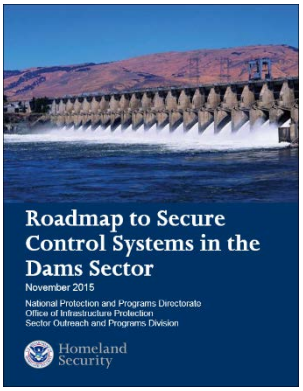
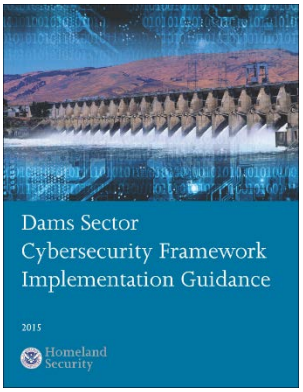
Dams Sector Cybersecurity Documents

The Dams Sector-Specific Agency has guided the development of five cybersecurity documents to aid the sector in its efforts to improve its cybersecurity preparedness and create a robust cybersecurity posture. To obtain these documents, please visit the Dams Sector Publications webpage at www.dhs.gov/dams-sector-publications or email dams@hq.dhs.gov.

2015 Roadmap to Secure Control Systems in the Dams Sector

A cyber event, whether caused by an external adversary, an insider threat, or inadequate policies and procedures, can initiate a loss of system control resulting in negative consequences. This Roadmap describes a plan and strategic vision for voluntarily improving the cybersecurity posture of control systems within the Dams Sector. It also highlights recommended strategies to address sector challenges, specifies mitigation requirements, and lists long-term research and development needs regarding control system security.



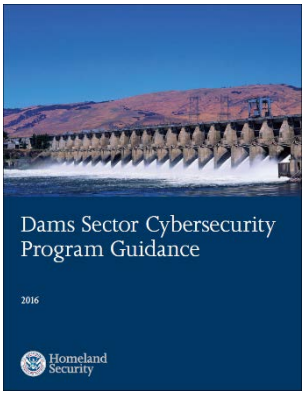


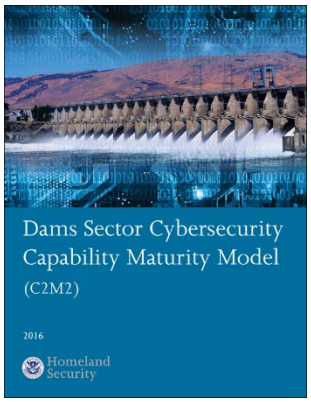
2015 Dams Sector Cybersecurity Framework Implementation Guidance

This guidance enables an organization—regardless of its size, degree of risk, or cybersecurity sophistication—to apply the principles and effective practices of cyber risk management to improve the security and resilience of its critical infrastructure. It recommends an approach that enables organizations to prioritize their cybersecurity decisions based on individual business needs without additional regulatory requirements.

2016 Dams Sector Cybersecurity Program Guidance

This guidance outlines various strategies and methods to develop or improve a basic cybersecurity program, enabling owners and operators to select cybersecurity activities and measures appropriate to their cyber assets and risk profiles, including Industrial Control Systems (ICS). These guidelines assist Dams Sector owners and operators of any size in characterizing their current and target cybersecurity postures; identifying gaps in their existing cybersecurity risk management efforts; recognizing existing Sector tools, standards, and guidelines that support cyber risk management; effectively demonstrating and communicating their risk management approaches to both internal and external stakeholders; and assisting in the implementation of relevant Cybersecurity Framework elements.

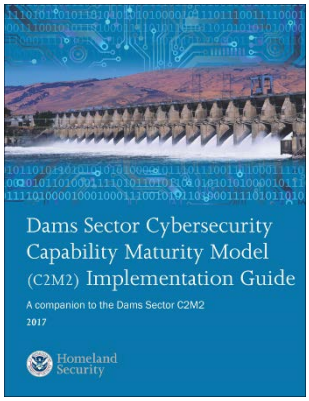




2016 Dams Sector Cybersecurity Capability Maturity Model (C2M2)

This model improves cybersecurity risk management across the Dams Sector by providing all Dams Sector organizations, regardless of size or type, with a flexible tool to help them evaluate, prioritize, and improve their cybersecurity capabilities. The model is organized into 10 domains, each containing a logical grouping of structured cybersecurity practices. Together these domains and practices describe a robust program for cybersecurity and risk management. The model may be used to identify an approach to building strong cybersecurity capabilities, evaluate capabilities in an organized way, prioritize actions, and measure progress toward goals.

2017 Dams Sector Cybersecurity Capability Maturity Model Implementation Guide



A supplement to the Dams Sector Cybersecurity Capability Maturity Model (C2M2), this guidance addresses the systematic implementation and management of cybersecurity practices associated with information technology and operations technology assets and the environments in which they operate. The guide highlights approaches to implementing both the administrative and substantive elements of each of the five steps of the C2M2, taking into account the actions and perspectives of the organization, facilitator, and participants. The approaches are presented as considerations, ranging from simple to complex, which can be selected by the organization based on its structure; available personnel and financial resources; and current processes related to planning, gap analysis, and project management.

Contact Information

For more information about the Dams Sector cybersecurity documents, please contact dams@hq.dhs.gov.