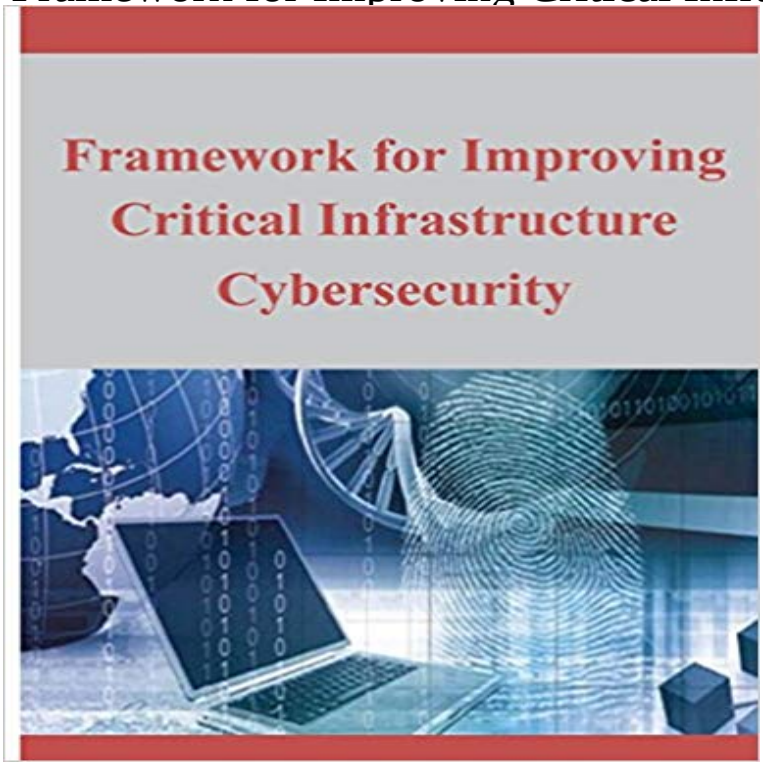
Framework for Improving Critical Infrastructure Cybersecurity



The national and economic security of the United States depends on the reliable functioning of critical infrastructure. To strengthen the resilience of this infrastructure, President Obama issued Executive Order 13636 (EO), Improving Critical Infrastructure Cybersecurity, on February 12, 2013.1 This Executive Order calls for the development of a voluntary Cybersecurity Framework (Framework) that provides a prioritized, flexible, repeatable, performance-based, and cost-effective approach to manage cybersecurity risk for those processes, information, and systems directly involved in the delivery of critical infrastructure services. The Framework, developed in collaboration with industry, provides guidance to an organization on managing cybersecurity risk. Critical infrastructure is defined in the EO as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. Due to the increasing pressures from external and internal threats, organizations responsible for critical infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk. This approach is necessary regardless of an organizations size, threat exposure, or cybersecurity sophistication today. The critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nations infrastructure. Members of each critical infrastructure sector perform functions that are supported by information technology (IT) and industrial control systems (ICS).2 This reliance on technology, communication, and the interconnectivity of IT and ICS has changed and expanded

the potential vulnerabilities and increased potential risk to operations. For example, as ICS and the data produced in ICS operations are increasingly used to deliver critical services and support business decisions, the potential impacts of a cybersecurity incident on an organizations business, assets, health and safety of individuals, and the environment should be considered. To manage cybersecurity risks, a clear understanding of the organizations business drivers and security considerations specific to its use of IT and ICS is required. Because each organizations risk is unique, along with its use of IT and ICS, the tools and methods used to achieve the outcomes described by the Framework will vary. Recognizing the role that the protection of privacy and civil liberties plays in creating greater public trust, the Executive Order requires that the Framework include a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities. Many organizations already have processes for addressing privacy and civil liberties. The methodology is designed to complement such processes and provide guidance to facilitate privacy risk management consistent with an organizations approach to cybersecurity risk management. Integrating privacy and cybersecurity can benefit organizations by increasing customer confidence, enabling more standardized sharing of information, and simplifying operations across legal regimes.

Comments on Draft Update of the Framework for Improving Critical The national and economic security of the United States depends on the reliable functioning of critical infrastructure. Cybersecurity threats take **Home Framework for Improving Critical Infrastructure Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity - NIST** Proposed Update to the Framework for Improving Critical Infrastructure Cybersecurity. A Notice by the National Institute of Standards and **Framework for Improving Critical Infrastructure Cybersecurity - NIST** This letter regarding proposed updates to the Framework for Improving Critical Infrastructure Cybersecurity was sent to Edwin Games at the **Framework for Improving Critical Infrastructure Cybersecurity** Improving Critical Infrastructure Cybersecurity. It is the policy of the United States to enhance the security and resilience of the Nations critical infrastructure and **Proposed Changes to the NIST Cybersecurity Framework Insights** Framework for Improving. Critical Infrastructure Cybersecurity. Draft Version 1.1. National Institute of

Standards and Technology. January 10 **Cybersecurity Framework for Improving Critical Infrastructure What** (Draft) Cybersecurity Framework v1.1 (PDF) with markup (Draft) Cybersecurity Framework v1.1 (PDF) without markup (Draft) Cybersecurity **Framework for Improving Critical Infrastructure Cybersecurity - NIST** Cybersecurity Framework a set of industry standards and best practices to improving the security and resilience of critical infrastructure. **NIST Releases Update to Cybersecurity Framework NIST** Improving Critical Infrastructure Cybersecurity. It is the policy of the United States to enhance the security and resilience of the Nations critical infrastructure and **Framework for Improving Critical Infrastructure Cybersecurity** The NIST Cybersecurity Framework (NIST CSF) provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, by the US National Institute of Standards and Technology in 2014, originally aimed at operators of critical infrastructure. Is being **US Chamber Letter to NIST on Proposed Updates to the Framework** Framework for Improving. Critical Infrastructure Cybersecurity. Draft Version 1.1. National Institute of Standards and Technology. January 10 **Proposed Update to the Framework for Improving Critical** PDS Implementation of the NIST Framework for Improving Critical Infrastructure Cybersecurity - V 1.0 NIST - February 12, 2014 **Framework for Improving Critical Infrastructure Cybersecurity** Improving Critical Infrastructure Cybersecurity. It is the policy of the United States to enhance the security and resilience of the Nations critical infrastructure and **Critical Infrastructure Cybersecurity - National Institute of Standards** Cybersecurity Framework for Improving Critical Infrastructure. What Others are Saying. Table of Contents. Energy Companies. **Cybersecurity Framework NIST** Re: Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity. On behalf of the close to 200 members of **Cybersecurity Framework NIST** Cybersecurity Framework a set of industry standards and best practices to improving the security and resilience of critical infrastructure. **Framework for Improving Critical Infrastructure Cybersecurity - NIST** Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure. **NIST Cybersecurity Framework - Wikipedia** In February 2013, President Obama signed Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity. One of the major **Cybersecurity Framework Draft Version 1.1 NIST** Improving Critical Infrastructure Cybersecurity, in February 2013. NIST continues to welcome informal feedback about the Framework and **Background: Framework for Improving Critical Infrastructure - NIST** The 2017 draft Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 incorporates feedback since the release of framework **NIST Framework For Improving Critical Infrastructure Cybersecurity** Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure. **NIST updates Framework for Improving Critical Infrastructure** Created through collaboration between industry and government, the Framework for Improving Critical Infrastructure Cybersecurity consists of standards, **NIST Framework for Improving Critical Infrastructure Cybersecurity** Improving Critical Infrastructure Cybersecurity. It is the policy of the United States to enhance the security and resilience of the Nations critical infrastructure and **Improving Critical Infrastructure Cybersecurity Executive Order 13636** The NIST Cybersecurity Framework is one of the most robust set of in the Framework for Improving Critical Infrastructure Cybersecurity. **Framework for Improving Critical Infrastructure Cybersecurity - NIST Using the Cybersecurity Framework Homeland Security** How can you streamline and improve conformance with NIST CSF technical controls? The NIST Cybersecurity Framework (CSF) is gaining broad acceptance as **Framework for Improving Critical Infrastructure Cybersecurity** The National Institute of Standards and Technology (NIST) issued an update to its Framework for Improving Critical Infrastructure Cybersecurity **News for Framework for Improving Critical Infrastructure Cybersecurity** The original goal was to develop a voluntary framework to help organizations manage cybersecurity risk in the nations critical infrastructure but Improving Critical Infrastructure Cybersecurity. It is the critical infrastructure and to maintain a cyber The Cybersecurity Framework Is for Organizations 6. **Harness the Power of the NIST Cybersecurity Framework** Framework for Improving. Critical Infrastructure Cybersecurity. Draft Version 1.1. National Institute of Standards and Technology. January 10