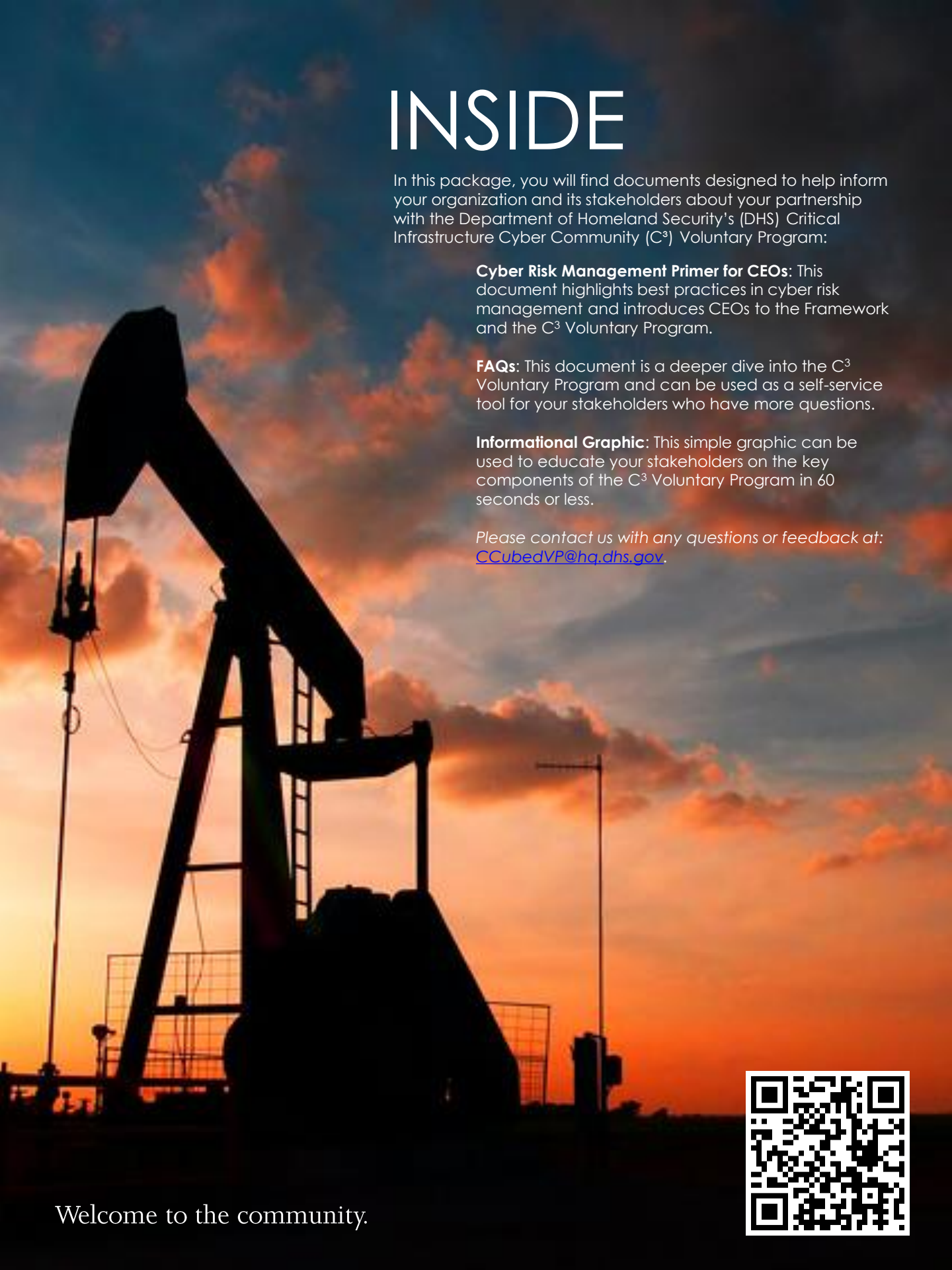
C3 VOLUNTARY PROGRAM

OUTREACH & MESSAGING KIT

Welcome to the community.

dhs.gov/ccubedvp

#ccubedvp



INSIDE

In this package, you will find documents designed to help inform your organization and its stakeholders about your partnership with the Department of Homeland Security's (DHS) Critical Infrastructure Cyber Community (C^3) Voluntary Program:

Cyber Risk Management Primer for CEOs: This document highlights best practices in cyber risk management and introduces CEOs to the Framework and the C^3 Voluntary Program.

FAQs: This document is a deeper dive into the C^3 Voluntary Program and can be used as a self-service tool for your stakeholders who have more questions.

Informational Graphic: This simple graphic can be used to educate your stakeholders on the key components of the C^3 Voluntary Program in 60 seconds or less.

Please contact us with any questions or feedback at: CCubedVP@hq.dhs.gov.

Welcome to the community.

C3 VOLUNTARY PROGRAM

Cyber Risk Management Primer for CEOs of Small & Midsize Businesses

Technology has advanced at an exponential rate and your mission increasingly relies on technology. As the CEO of a small or midsize business (SMB), you understand that any disruption to your information systems can hamper your operations, slow your supply chain, impact your reputation, compromise sensitive customer data or intellectual property, and ultimately hurt your bottom line.

And this is not just a big business problem. From 2012 to 2013 there was a 300% increase in cyber attacks on small businesses. It's true that SMB are all in different stages of maturity, but they also all possess extremely valuable data.

In your seat, it is imperative that you protect your systems from cyber threats—the lifeblood of your business depends on it.

5 Questions CEOs of SMB Should Ask about Cyber Risks

1) What is the current level and business impact of cyber risks to our company? What is our plan to address identified risks?
2) How is our leadership team informed about the current level and business impact of cyber risks to our company?
3) Does our business have a cybersecurity program? How does that program apply industry standards and best practices?
4) How many and what types of cyber incidents do we detect on a regular basis? What is the threshold for notifying our leadership team?
5) How comprehensive is our cyber incident response plan? How often is the plan tested?

Key Cyber Risk Management Concepts

Incorporate cyber risks into existing risk management and governance processes.

Cybersecurity is about more than implementing a checklist of requirements—cybersecurity is managing cyber risks to an ongoing and acceptable level.

Begin cyber risk management discussions with your leadership team.

Communicate regularly with those accountable for managing cyber risks. Enhance your awareness of current risks affecting your organization and associated business impact. Discuss the pros and cons of outsourcing cybersecurity services, if necessary.

Implement industry standards and best practices. Don't rely on compliance.

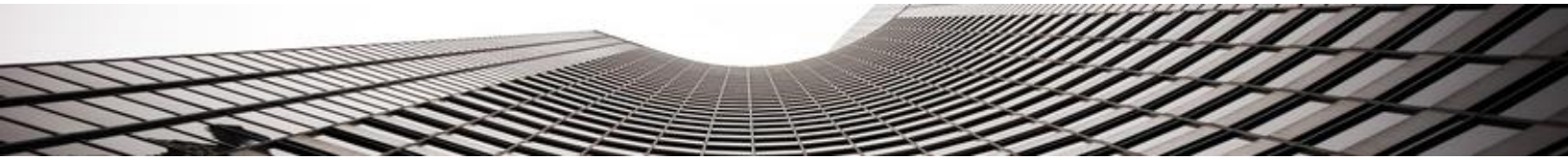
A comprehensive cybersecurity program leverages industry standards and best practices to protect systems and detect potential problems. It informs processes of new threats and enables timely response and recovery.

Evaluate and manage specific cyber risks.

Identifying critical assets and associated impacts from cyber threats is essential to understanding an organization's risk exposure–whether financial, competitive, reputational, or regulatory. Risk assessment results are essential for identifying and prioritizing specific protective measures, allocating resources, informing long-term investments, and developing policies and strategies to manage cyber risks.

Provide oversight and review.

Executives are responsible for managing and overseeing enterprise risk management. Cyber oversight activities include the regular evaluation of cybersecurity budgets, information technology (IT) acquisition plans, IT outsourcing, cloud services, incident reports, risk assessment results, and top-level policies.



Develop and test incident response plans and procedures.

Even a well-defended business will experience a cyber incident at some point. When network defenses are penetrated, a CEO should be prepared to answer, "What is our Plan B?" Cyber incident response plans should be exercised regularly.

Coordinate cyber incident response planning across the enterprise.

Early response actions can limit or even prevent possible damage and require coordination with your organization's leaders and stakeholders. This includes your Chief Information Officer, Chief Information Security Officer, Chief Security Officer, business leaders, continuity planners, system operators, general counsel, public affairs, and human resources. Integrate cyber incident response policies and procedures with existing disaster recovery and business continuity plans.

Maintain awareness of cyber threats.

Situational awareness of an organization's cyber risk environment involves timely detection of cyber incidents, along with the awareness of current threats and vulnerabilities specific to that organization and associated business impacts. Analyzing, aggregating, and integrating risk data from various sources and participating in threat information sharing with partners helps organizations identify and respond to incidents quickly and helps organizations to ensure that protective efforts are commensurate with the risks.

How the Framework Can Help

As directed by Executive Order (E.O.) 13636, the National Institute of Standards and Technology (NIST) has developed a Cybersecurity Framework that your company can use to apply the principles and best practices of risk management to reduce your cyber risk while enhancing your resilience. By providing a common structure for defining your cybersecurity profile, the Framework will help you identify and understand your company's dependencies on your business partners, vendors, and suppliers. As part of an enterprise approach to risk management, the Framework provides, for the first time, a common language to address and manage cyber risk as a mission equal in priority to other risk areas, such as financial and reputational risk.

For more information on the Framework, please visit: www.nist.gov/cyberframework.

Join the C³ Voluntary Program

Interested in using the Cybersecurity Framework within your company? Join the **Critical Infrastructure Cyber Community (C³, pronounced C-Cubed) Voluntary Program**.

DHS created the C³ Voluntary Program to provide guidance and offer technical assistance and other resources and tools to aid companies in implementing the Framework.

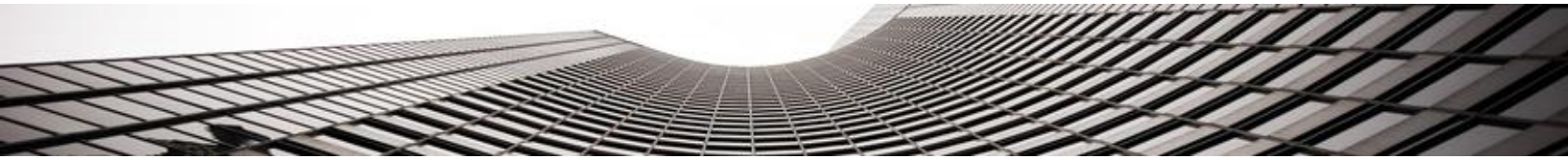
The **C³ Voluntary Program** will be the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes and will: **1)** support industry in increasing cyber resilience; **2)** increase awareness and use of the Framework; and **3)** encourage companies to manage cybersecurity as part of their approach to enterprise risk management.

For more information, please visit: www.dhs.gov/ccubedvp.

To learn about DHS's role supporting enterprise risk management across critical infrastructure, visit: www.dhs.gov/critical-infrastructure.

For more information about DHS's role in securing the Nation's cyber ecosystem, please visit: www.dhs.gov/cyber.

To report a cyber-incident, please visit www.forms.us-cert.gov/report or call (888) 282-0870.



C³ VOLUNTARY PROGRAM | Frequently Asked Questions

Welcome to the community.

About the C³ Voluntary Program

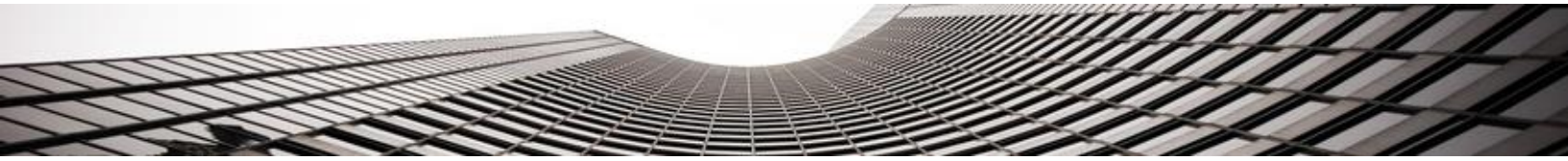
What is the Critical Infrastructure Cyber Community (C³) Voluntary Program?
The C³ (pronounced "C-Cubed") Voluntary Program is a public-private partnership aligning business enterprises as well as Federal, State, Local, Tribal, and Territorial (SLTT) governments to existing resources that will assist their efforts to use the National Institute of Standards and Technology (NIST) Cybersecurity Framework to manage their cyber risks as part of an all-hazards approach to enterprise risk management.

Why is there a need for a voluntary program?
Currently, there are many programs and resources available to critical infrastructure sectors and organizations that are looking to improve their cyber risk resilience. These resources are provided by many DHS and government-wide agencies and offices. The C³ Voluntary Program provides the central place to access that information. The C³ Voluntary Program will be the coordination point within the Federal Government to leverage and enhance existing capabilities and resources to promote use of the Cybersecurity Framework.

And while the Cybersecurity Framework is based on existing guidelines and standards, organizations still need assistance in understanding its purpose, and how the Framework might apply to them. The C³ Voluntary Program will provide assistance to organizations of all types interested in using the Cybersecurity Framework.

What will the C³ Voluntary Program do?
The C³ Voluntary Program will focus on three main activities:

- **Use:** Assist stakeholders with understanding use of the Cybersecurity Framework and other cyber risk management efforts, and support development of general and sector-specific adoption guidance.
- **Outreach and Communications:** Serve as a link and customer relationship manager to help organizations with Framework use, and guide interested organizations and sectors to DHS and other public and private sector resources to support use of the Cybersecurity Framework.
- **Feedback**: Encourage feedback from stakeholder organizations about their experience using C³ Voluntary Program resources to implement the Framework. The C³ Voluntary Program works with organizations to understand how they are using the Framework, and to receive feedback on how the Framework and the C³ Voluntary Program can be improved to better serve



organizations. Feedback about the Framework will also be shared with NIST, to help guide the development of the next version of the Framework.

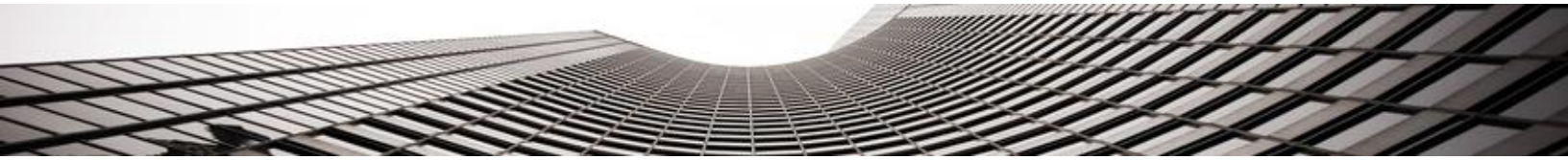
How does the C³ Voluntary Program align with the updated National Infrastructure Protection Plan (NIPP)?
The C³ Voluntary Program's approach to sectors and the Cybersecurity Framework is aligned with the process and efforts outlined in the 2013 NIPP. The C³ Voluntary Program will work with the DHS Office of Infrastructure Protection to incorporate use of the Cybersecurity Framework and participation in the C³ Voluntary Program into sector-specific reporting guidance. The C³ Voluntary Program will provide resources to support use of the Cybersecurity Framework, and will work with each sector to develop sector-specific implementation guidance, if needed.

Participating in the C³ Voluntary Program

What are the benefits of participating in the C³ Voluntary Program?
The C³ Voluntary Program provides support to all business enterprises looking to enhance their cyber risk resilience. This includes providing tailored guidance on how to use the Cybersecurity Framework. Other benefits include:

- The ability to participate in forums for knowledge sharing and collaboration related to Cybersecurity Framework use. Over time, DHS plans to work with the private sector to encourage the development of communities of interest for the C³ Voluntary Program
- Access to freely available technical assistance, tools, and resources to strengthen capabilities to manage cyber risks
- Opportunities to influence peers and other partners in the critical infrastructure community
- Assistance with meeting fiduciary responsibilities to manage cyber risks, in a consistent way with others in critical infrastructure that can aid in communication internally and externally

My organization is interested in working with the C³ Voluntary Program. How do we get started?
There are several ways to participate in the C³ Voluntary Program. Interested organizations can work through their Sector Specific Agencies (SSAs) or Sector Coordinating Councils (SCCs) to express interest in developing or accessing sector-specific guidance for using the Cybersecurity Framework. Organizations can also visit www.us-cert.gov/ccubedvp to download a Cyber Resilience Review or learn more about existing DHS resources.



Can you use the Cybersecurity Framework and not participate in the C³ Voluntary Program?
Organizations are encouraged to use the Cybersecurity Framework as they see fit and on their own time. The C³ Voluntary Program is available to help any organization that needs assistance in using the Cybersecurity Framework or with other cyber risk management efforts.

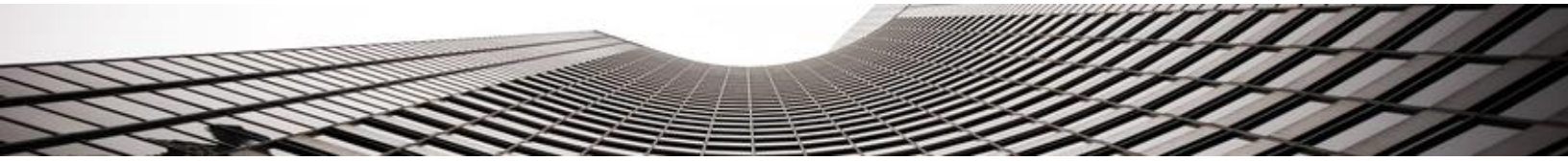
How does an organization access existing DHS resources?
The C³ Voluntary Program has developed web pages that provide a central location for resources that can be leveraged for Cybersecurity Framework use. These tools include DHS resources and programs, as well as cross-sector, SLTT government, and private sector resources. Once an organization identifies a resource they are interested in leveraging, they can work with the C³ Voluntary Program to connect to the office or program that manages that resource.

What is the Cyber Resilience Review?
The Cyber Resilience Review (CRR) is a no-cost, voluntary, non-technical assessment to evaluate an organization's information technology resilience. The CRR may be conducted as a self-assessment or as an in-person facilitated assessment. The goal of the CRR is to develop an understanding and measurement of key capabilities to provide meaningful indicators of an organization's operational resilience and ability to manage cyber risk to its critical services during normal operations and times of operational stress and crisis. The CRR has been designed to be applicable to public and private organizations within all critical infrastructure sectors and has also been designed to accommodate a wide variety of sizes and organizational structures.

Will the C³ Voluntary Program share information about my organization with other government agencies?
The C³ Voluntary Program will not share information about your organization with other government agencies. Any information received by the C³ Voluntary Program will be used to share general lessons learned and benefits, and to improve the quality or delivery of existing resources.

Cybersecurity Framework

Who "owns" the Cybersecurity Framework?
The National Institute for Standards and Technology (NIST) will continue to lead revisions to the Cybersecurity Framework. The purpose and focus of the C³ Voluntary Program is to help increase organizations' use of cyber risk management processes, primarily by supporting their use of the Framework and conducting outreach and engagement around available resources. As part of this effort, the C³ Voluntary Program will receive feedback from program participants about their use of



program resources. If participants offer feedback on the Framework, the C³ Voluntary Program will forward this information to NIST, as NIST will lead the development of the next iteration of the Framework.

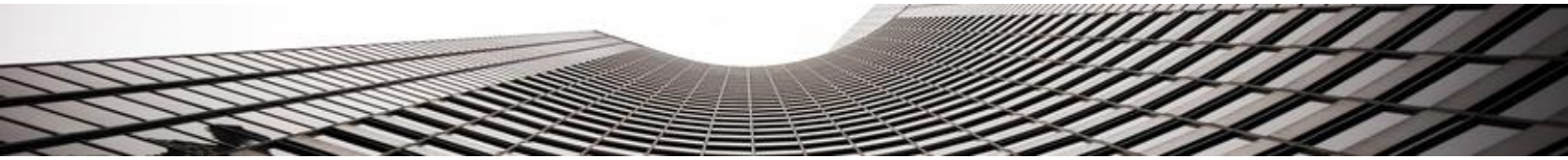
What does it mean to "use" the Cybersecurity Framework?
Using the Cybersecurity Framework will look different for every organization. There is no "right" or "complete" way to use the Framework, and NIST and DHS are not going to validate whether or not an organization has used the Framework. In general, any organization that uses the Framework as a part of its process to identify and manage cyber risk has "used" the Framework.

Why is DHS interested in knowing how an organization is using the Cybersecurity Framework?
DHS will encourage voluntarily-provided feedback from organizations that are using DHS and government resources to enhance their cyber resilience. This includes organizations who are taking advantage of these resources to support their use of the Cybersecurity Framework. This feedback will help DHS identify lessons learned, benefits, and improvements to existing resources.

My organization already complies with industry-wide regulatory requirements. Can I apply our regulatory compliance activities towards adopting the Cybersecurity Framework?
DHS understands that organizations may use a wide range of activity towards practicing cyber risk management. Because of this, there will be different methods and approaches to using the Cybersecurity Framework. As part of its initial phase of engagement, the C³ Voluntary Program will support each sector as sectors develop tailored guidance, taking into account each sector's unique combination of threats, business needs, and legal and regulatory environments.

How will use of the Cybersecurity Framework be measured?
Entities will measure their own progress against their desired outcomes. For entities that were identified during the EO 13636 Section 9: Cyber Dependent Critical Infrastructure process, SSAs will work with those entities to understand how they are using the Cybersecurity Framework.

Will I be able to display a cybersecurity emblem or sticker at my business if I use the Cybersecurity Framework or participate in the C³ Voluntary Program?
The C³ Voluntary Program is not going to validate whether or not any organization is using the Cybersecurity Framework. The purpose and focus of the C³ Voluntary Program is to encourage organizations to implement a cyber risk management process, primarily by supporting use of the Cybersecurity Framework and conducting outreach and engagement around available resources.



If a cyber incident occurs and a customer sues my company, how can I prove that I am using the Cybersecurity Framework?
The C³ Voluntary Program is not going to validate whether or not any organization is using the Cybersecurity Framework. The purpose and focus of the C³ Voluntary Program is to encourage organizations to implement a cyber risk management process, primarily by supporting use of the Cybersecurity Framework and conducting outreach and engagement around available resources.

Incentives

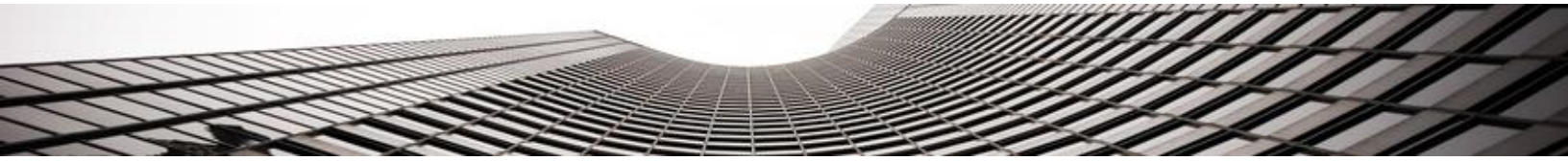
What incentives will be offered for the Cybersecurity Framework?
EO 13636 orders the establishment of a set of incentives designed to promote participation in the program. The types of incentives to be offered are still under consideration, and include cybersecurity insurance, grants, process preference, liability limitation, streamline regulations, public recognition, rate recovered for price regulated industries, and cybersecurity research.

How do I access the incentives to adopt the Cybersecurity Framework?
Potential incentives are currently undergoing review. When incentives are finalized, organizations will work directly with the department or agency providing the incentive.

How would my organization engage with the C³ Voluntary Program to demonstrate we are using the Cybersecurity Framework in order to qualify for incentives?
The C³ Voluntary Program is not going to validate whether or not any organization is using the Cybersecurity Framework. An organization will have to work with the agency tasked with overseeing that incentive to determine if the organization does or does not qualify. The C³ Voluntary Program is a convening mechanism for discussions about incentives, but has no role in the issuance of incentives.

About Executive Order 13636 and Presidential Policy Directive 21

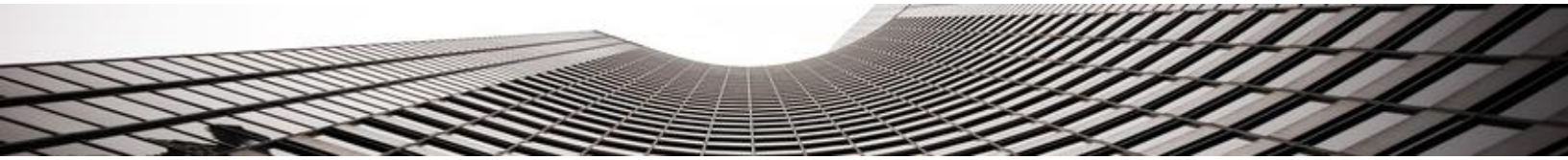
What is the Executive Order 13636 and Presidential Policy Directive 21?
On February 12, 2013, President Obama signed the Executive Order (EO) 13636: *Improving Critical Infrastructure Cybersecurity* (http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity) to strengthen the cybersecurity of critical infrastructure by increasing information sharing and by jointly developing and implementing a framework of cybersecurity practices with industry partners. The Administration also issued Presidential Policy Directive (PPD) 21: *Critical Infrastructure Security and Resilience* (http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-



infrastructure-security-and-resil), which acknowledges the increased role of cybersecurity in securing physical assets and will help strengthen the security and resilience of the Nation's critical infrastructure against all hazards. Read the Department of Homeland Security's fact sheet on the EO and the PPD here: http://www.dhs.gov/news/2013/02/13/fact-sheet-executive-order-cybersecurity-presidential-policy-directive-critical.

How are the EO and PPD being implemented?

The EO directs the Federal Government to use a consultative process to address cybersecurity for critical infrastructure and continue to engage public-private partnerships. While DHS has several key roles in the executive of the EO and PPD, the ultimate success will be determined by how well the Federal Government and critical infrastructure owners and operators collaborate to implement the strategy and tactics necessary to improve the Nation's cybersecurity posture. Federal Government and critical infrastructure owner and operator collaboration efforts will be facilitated under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework.



C³ VOLUNTARY PROGRAM

In February 2013, the President signed Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity and* Presidential Policy Directive (PPD)—21 *Critical Infrastructure Security and Resilience.* The EO and PPD represent an integrated approach that strengthens the security and resilience of critical infrastructure against all hazards through an updated national framework that acknowledges the evolving risk environment and increased role of cybersecurity in securing physical assets.

As part of the EO, the U.S. Department of Homeland Security (DHS) created the ***Critical Infrastructure Cyber Community (C³, pronounced C-Cubed) Voluntary Program*** to help improve the resilience of critical infrastructure cybersecurity systems by supporting and promoting the use of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework.

The ***C³ Voluntary Program*** is the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes. The (C³) Voluntary Program will:

1) Support industry in increasing its cyber resilience;
2) Increase awareness and use of the Framework; and
3) Encourage organizations to manage cybersecurity as part of an all hazards approach to enterprise risk management.

Critical Infrastructure

Ranging from emergency services and transportation systems to small and midsize businesses, U.S. critical infrastructure provides the essential services that underpin American society.

C³

Administration Policies

EO 13636 highlights the need for improved cybersecurity among critical infrastructure. PPD-21 calls for efforts to strengthen the physical and cyber security and resilience of our Nation's critical infrastructure.

Cybersecurity Framework

One of the major components of the EO is the development of the Framework by NIST to help critical infrastructure sectors and organizations reduce and manage their cyber risk as part of their approach to enterprise risk management.

Welcome to the community.

dhs.gov/ccubedvp

#ccubedvp