C3 VOLUNTARY PROGRAM

CRITICAL INFRASTRUCTURE CYBER COMMUNITY VOLUNTARY PROGRAM

CYBER COMMUNICATION RESOURCES

WELCOME TO THE COMMUNITY.

#ccubedvp

CYBER COMMUNICATION RESOURCES

Overview

The **Critical Infrastructure Cyber Community (C^3) Voluntary Program** launched in February 2014 in support of Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity. Among other actions, the EO charged the National Institute of Standards and Technology (NIST) with the development of a Cybersecurity Framework to help critical infrastructure sectors and organizations reduce and manage their cyber risk. The C^3 Voluntary Program supports owners and operators of critical infrastructure and any other interested entities in the use of Framework to address and improve their cybersecurity and risk management. For more information, please contact us at ccubedvp@hq.dhs.gov or visit our website, www.us-cert.gov/ccubedvp.

The more resilient critical infrastructure becomes, the more resilient our Nation becomes. And that resilience begins at the organization and community level. So we are relying on you, our stakeholders and partners, to help us get the word out in your organizations and communities about your involvement with the C^3 Voluntary Program; your use of the Framework; and all the tools and resources available to help organizations use the Framework.

We have created a series of draft messages to help you promote your organization's involvement with the C^3 Voluntary Program, as well as your commitment to cybersecurity risk management within your own organization, to your stakeholders, employees, and partners. By working together, we can inspire a nationwide culture around cybersecurity and risk management.

Content

In this document, you will find the following templates and resources, which explain the C^3 Voluntary Program and announce your organization's commitment to cyber risk management:

Social Media Samples...2
- Blog post
- Facebook post
- Tweets (Twitter) with suggested relevant hashtags
- C^3 Voluntary Program's website QR code

Sample Leadership Message for CEOs...4
Sample Newsletter Article for CEOs..5

CYBER COMMUNICATION RESOURCES

Social Media Samples

[Please contact ccubedvp@hq.dhs.gov to notify the C³ Voluntary Program of the use of this template.]

The **C³ Voluntary Program** uses several social media platforms through DHS:

TWITTER	FACEBOOK	BLOG
• @Cyber	• Homeland Security	• The Blog @ Homeland Security

Your organization can use social media vehicles to promote your use of the Framework and provide your colleagues with information on how to obtain tools and resources to use the Framework in their organizations.

On subsequent pages, find sample social media content to announce your organization's involvement with the **C³ Voluntary Program**.

CYBER COMMUNICATION RESOURCES

BLOG POST

[Organization] Joins the DHS C^3 Voluntary Program

[Organization] is pleased to announce our collaboration with the Department of Homeland Security's (DHS) **Critical Infrastructure Cyber Community (C^3) Voluntary Program** to aid in our use of the national Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST). The Framework, a crucial piece of Executive Order 13636, will help us to further reduce and manage our cyber risk and interact with other members of the critical infrastructure community using a common language to describe our cyber risks.

DHS is responsible for safeguarding our Nation's critical infrastructure from physical and cyber threats that can affect our national security, public safety, and economic prosperity. The **C^3 Voluntary Program** was launched to provide guidance and offer technical assistance and other resources and tools to aid companies in using the Framework.

The **C^3 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 **C^3 Voluntary Program** aims to: **1)** support industry in increasing 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.

Check back to see how [Organization] is working with the **C^3 Voluntary Program** to make the Nation more resilient at [Insert organization's Intranet or website URL]. To learn more about the **C^3 Voluntary Program**, visit: http://www.us-cert.gov/ccubedvp.

CYBER COMMUNICATION RESOURCES

FACEBOOK POSTS

- Proud to join the U.S. Department of Homeland Security’s C³ Voluntary Program to help improve our Nation’s critical infrastructure resilience and reduce cyber risk. Get more info at [Insert link to organization's website, press release, etc.]
- Learn more about [Organization]’s new involvement with the U.S. Department of Homeland Security’s C³ Voluntary Program here [Insert link to organization's website, press release, etc.]

TWITTER POSTS

- @[Organization handle] joins #ccubedvp to help improve our Nation’s critical infrastructure resilience and reduce #cyber risk
- #Cybersecurity is a shared responsibility & we each have a role to play. Learn more about our involvement with #ccubedvp [Insert shortened URL to your website, press release, etc.]

RELEVANT HASH TAGS

- #ccubedvp; #cybersecurityframework
- #cyber; #online; #cybersecurity; #criticalinfrastructure

QR CODE TO WEBSITE (dhs.gov/ccubedvp)

CYBER COMMUNICATION RESOURCES

Sample Leadership Message for CEOs

[Please contact ccubedvp@hq.dhs.gov to notify the C³ Voluntary Program of the use of this template.]

[Insert text below on your organization's letterhead]

[Date]

Dear Colleagues,
As technology evolves, [organization] has become more reliant on cyber-dependent technology than ever before. Our systems help to make our operations more efficient and help us to scale our efforts to serve more people. With this increased dependence on technology comes an increased cyber threat, which we work very hard to combat every day.

To enhance our efforts, [organization] has partnered with the U.S. Department of Homeland Security's (DHS) Critical Infrastructure Cyber Community (C³) Voluntary Program. In February 2013, the President signed Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity, and one of the major components of the EO was the development of a Cybersecurity Framework by the National Institute of Standards and Technology (NIST) to help organizations like us reduce and manage cyber risk.

The EO also initiated the creation of a voluntary program, led by DHS, to serve as the coordination point between the critical infrastructure sectors and the Federal Government to help organizations improve their cyber risk management processes. The purpose of the C³ Voluntary Program is: 1) to support industry in increasing cyber resilience; 2) to increase awareness and use of the Framework; and 3) to encourage organizations to manage cybersecurity as part of an all hazards approach to enterprise risk management.

For additional information about the C³ Voluntary Program, I encourage you to visit http://www.us-cert.gov-/ccubedvp. I look forward to this new endeavor and hope that each of you will do your part to advance this important issue.

Sincerely,
[Name]

CYBER COMMUNICATION RESOURCES

Sample Newsletter Article for CEOs

[Please contact ccubedvp@hq.dhs.gov to notify the C^3 Voluntary Program of the use of this template.]

[Insert text below on your organization’s letterhead]

[Organization] Joins the U.S. Department of Homeland Security’s Critical Infrastructure Cyber Community (C^3) Voluntary Program

[Date]

[Organization] recently joined the U.S. Department of Homeland Security’s (DHS) Critical Infrastructure Cyber Community (C^3) Voluntary Program, forming a new partnership that will link us to tools and resources to aid in our use of the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST). The Framework is a crucial piece of Executive Order 13636, which will help us to further reduce and manage our cyber risks and interact with other members of the critical infrastructure community using a common language to describe our cyber risks.

As technology evolves, [Organization] has become more reliant on cyber-dependent technology than ever before. Our systems help to make our operations more efficient and scale our efforts to serve more people. With this increased dependence on technology comes an increased cyber threat, which we work very hard to combat every day.

The C^3 Voluntary Program was launched by DHS to provide guidance and offer technical assistance and other resources and tools to aid organizations in implementing the Framework. DHS is responsible for safeguarding our Nation’s critical infrastructure from physical and cyber threats that can affect our national security, public safety, and economic prosperity.

The C^3 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 C^3 Voluntary Program aims to: 1) support industry in increasing its cyber resilience; 2) increase awareness and use of the Framework; and 3) encourage companies to manage cybersecurity as part of an all hazards approach to enterprise risk management.

Check back to see how [Organization] is working with the C^3 Voluntary Program to make the Nation more resilient at [Insert Organization's Intranet URL] . To learn more about the C^3 Voluntary Program, visit www.us-cert.gov/ccubedvp.

WELCOME TO THE COMMUNITY.

#ccubedvp

dhs.gov/ccubedvp