Carnegie Mellon University
Software Engineering Institute

A Guide to Effective Incident Management Communications

Brittany Manley
David McIntire

Contents

Introduction

This document provides cybersecurity centers and incident response teams with high-level guidance on effective communications planning, and considerations and best practices for communications responsibilities in support of incident response services. Communications, both in times of crisis and during normal operations, are essential to the overall success and sustainability of your team. You may be responsible for many different types of and mechanisms for communications—ranging from communications with your constituents to the sharing of information with the general public and the media. How you plan for and manage these communications and how they are received by your audience will influence your trustworthiness, reputation, and ultimately your ability to perform incident management services effectively.

Audience

The primary audience for this document includes

- leaders, managers, and team members of:
  - Computer Security Incident Response Teams (CSIRTs)
  - National CSIRTs or Cybersecurity Centers
  - Security Operations Centers (SOCs)
- operators and managers of Critical Information Infrastructure

Others will also find this document useful, particularly organizations and entities that interact with cybersecurity centers and CSIRTs when events and incidents occur. They include

- C-level executives
- stakeholders involved in the management of and response to cybersecurity events and incidents
- stakeholders responsible for cyber planning and policy development
- other information owners
- organizational public relations and/or communications stakeholders
- media outlets

How to Use This Document

We want this document to be a valuable resource for cybersecurity and incident response organizations looking to improve their communications planning and activities. This document will provide considerations for various types of communications that you may be responsible for, including communications with constituents, the general public, the media, and crisis communications. It will address communications best practices for the dissemination of timely and accurate information, including organizational considerations, types of communication and content, and examples of what should be included within communications plans. However, when using this document as a guide, be sure to tailor the information to your own organizations, services, and constituents accordingly.

Communications: Setting the Context

Communications are fundamental and critical elements of any team that provides incident response and coordination services to its constituency. Regardless of the need for effective communications or widespread recognition of the importance of communications, they are often overlooked in organizational planning and strategy—and become reactive in nature.

For cybersecurity centers and incident response teams, communications and outreach will play a particularly significant role in reaching constituents, sharing information, building relationships, and fostering trust. It is important to consider communications as a strategic initiative. Communications transcend all business and security processes, both those that occur under normal operations as well as during a crisis.

Communications Planning

Every organization should develop and implement its own communications plan. This plan should include considerations for both internal and external communication, organizational branding, and messaging for particular audiences and communications objectives.

Communications planning is an important piece of normal operations for cybersecurity centers or CSIRTs, and there may be many different communications plans based on the specific objectives of the communication. There may be a specific communications plan for internal information sharing (across CSIRT and SOC staff, for example) or sharing information with constituents. There may be a separate communications plan for sharing information with the general public or with the media. Another example of a communications plan might be a standalone *crisis* communications plan.

In any of these scenarios, communications, much like incident management, can be proactive or reactive. Ideally, communications planning and activities are conducted proactively, to prepare your organization in the event you need to activate a communications plan. Unfortunately, there may be times where your organization is forced to communicate reactively, in the middle of an incident or a crisis.

HAVE A REACTIVE PLAN IN PLACE

Having an established communications plan will benefit your organization's ability to handle incidents, while attempting to maintain its reputation, keep its message simple and consistent, and ensure accurate and timely information is released to the appropriate audience.

Communications Considerations

There are many organizational and governance considerations to account for when designing and implementing organizational communications plans.

Organizational and Governance Considerations

First, it is important that you understand the environment in which your organization or team operates. This graphic illustrates the factors to consider as part of your environment.

You must also understand the communication roles and responsibilities of the individuals in your organization. Roles and responsibilities for the design and implementation of communications plans should be clearly defined, as well as who has the authority to determine roles and designate responsibilities, and under which situations these roles and responsibilities may be activated. Teams will function and communicate more efficiently when there is a common understanding of individuals roles and responsibilities within the organizational or team architecture.

1 Constituents are organizations or entities that will be served by your organization/team (for example, those that have cybersecurity and incident response services provided to them).

2 Communities are a broader set of tangential and related organizations that have some relationship with your organization/team, but may not fit the definition of stakeholders or constituents. Examples may include, but are not limited to, local, regional, or international incident response organizations.

Other Key Considerations

For any communications plan, internal or external, during normal operations or in a crisis, there are additional key factors you must continually consider. The most significant of these considerations are the following:

MESSAGING

The internal and external messaging must be carefully considered. An organization must agree on and deliver one shared, consistent message. This message should resonate with the audience and align with the particular communications goals and objectives.

REPUTATION

Another significant consideration must be your organization's reputation. What information is shared—and with whom—will depend on many factors, including the expected harm or damage, regulatory compliance and reporting requirements, and cost efficiency. How and when information is disclosed, and how you handle the situation from a communications perspective, will ultimately affect your organization's reputation in the industry and community. It takes a significant amount of time to earn and build trust from constituents, but only a short time to lose that trust.

STAKEHOLDER MANAGEMENT

Transparency and honesty are critical in the event of an incident. Your organization should be as transparent as possible with its constituents, and be honest about what is known versus unknown at any given time. Rumors can spread quickly, both internally and externally; therefore, it is important to combat rumors with transparency and messaging to maintain control of the situation and respond and recover effectively.

ACCURACY AND TIMELINESS OF THE INFORMATION

Communicate often and regularly throughout the lifecycle of an incident, both internally and externally. Any information disclosed during an incident must be both *accurate and timely.* The timeliness of notifications is critical to stakeholder communication and management. It is also important to stick to the facts versus speculation; accuracy of the information will influence stakeholder confidence and organizational reputation.

Elements of Communications Planning

This section outlines the critical steps for communications planning and determining the foundational elements of any organizational communications activities. You must clearly determine and define the following in order to outline an effective communications plan:

- **establish the purpose**
- **determine the audience**
- **define roles and responsibilities**
- **understand and standardize the messaging**
- **establish communication channels**
- **determine methods of distribution**

Once these factors have been identified, your organization can begin drafting and documenting a communications plan (see Appendix B for example sections and inclusions); however, communications planning does not end with the plan development. Additional steps required to continually improve the plan's overall effectiveness are *training to the plan, testing the plan, and reviewing and refining the plan* over time.

The first time the plan is tested should not be in the middle of a cybersecurity incident. All key stakeholders should be trained. This training can be conducted as a tabletop exercise or walkthrough of the plan. The plan should also be tested through a real-time simulated scenario to determine if it was designed appropriately, or if there are any updates required. Stakeholders must ensure understanding of the following:

- ***When is the plan activated?***
- ***Who activates the plan?***
- ***Who speaks to whom and under what circumstances?***
- ***What is my responsibility?***

For crisis communications specifically, arrangements should be established with third-party security experts and/or public relations firms in advance, if desired or required. See *Communications Responsibilities: Crisis Management Support* for more information on crisis communications.

Following the test of the plan and/or after using the communications plan, it is important to conduct lessons learned in order to continue improving on the plan. The plan should incorporate anything learned from the test or real-time event. Organizations should also ensure that a review and audit of the plan, as well as training, are conducted regularly. Some example questions that can be asked during a lessons-learned session are the following:

- ***What was done, and in what timeframe?***
- ***How did it benefit our constituencies/customers?***
- ***Do our processes scale?***
- ***Was the communications plan effective?***
- ***Were roles and responsibilities clear?***

Communications Planning, Responsibilities, and Activities

Communications planning is integral to incident response and management. Cybersecurity centers, SOCs, and CSIRTs must weave communications into their designated and advertised services. There are two frameworks highlighted below—the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and the Forum of Incident Response and Security Teams (FIRST) CSIRT Services Framework—that address the importance of communications, both in normal operations and during times of crises. These are provided as both additional considerations (for the types of communications your organization may be responsible for) and frameworks with which to integrate. These frameworks will also serve as a means to organize the communications responsibilities associated with *standard incident response activities,* and those communications responsibilities associated with *crisis management communications*.

NIST Cybersecurity Framework

NIST's Framework for Improving Critical Infrastructure Cybersecurity, otherwise known as the Cybersecurity Framework (CSF), has been applied by U.S. federal agencies, academia, small and medium sized businesses, and many international organizations and governments. The CSF was developed to "guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management process,"[3] and while designed to be implemented in critical infrastructure, the CSF has been applied across various sectors and communities.

The CSF identifies critical cybersecurity activities, otherwise known as the five functions of the CSF: Identify, Protect, Detect, Respond, and Recover. Communications are considered categories of the respond and recover functions. Your organization must therefore consider communications as an integral part of any incident management lifecycle and critical for the response to and recovery from any cybersecurity incident.

Communications Subcategories within the **respond** function address roles and responsibilities, consistency of shared information, and coordination and information sharing with stakeholders to improve on situational awareness.

Communications Subcategories of the **recover** function include public relations management, considerations for organizational reputation, and communication of recovery activities with all stakeholders involved.

3 **nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf**

Communications Categories

FUNCTION	CATEGORY UNIQUE IDENTIFIER	CATEGORY
IDENTIFY	**ID.AM**	Asset Management
	ID.BE	Business Environment
	ID.GV	Governance
	ID.RA	Risk Assessment
	ID.RM	Risk Management Strategy
	ID.SC	Supply Chain Risk Management
PROTECT	**PR.AC**	Identity Management and Access Control
	PR.AT	Awareness and Training
	PR.DS	Data Security
	PR.IP	Information Protection and Process Procedures
	PR.MA	Maintenance
	PR.PT	Protective Technology
DETECT	**DE.AE**	Anomalies and Events
	DE.CM	Security Continuous Monitoring
	DE.DP	Detection Processes
RESPOND	**RS.RP**	Response Planning
	RS.CO	**Communications**
	RS.AN	Analysis
	RS.MI	Mitigation
	RS.IM	Improvements
RECOVER	**RC.RP**	Recovery Planning
	RC.IM	Improvements
	RC.CO	**Communications**

Communications Categories Within the Respond and Recover Functions of the NIST CSF

CATEGORY	SUBCATEGORY
Communications (RS.CO) Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1** Personnel know their roles and order of operations when a response is needed
	RS.CO-2 Incidents are reported consistent with established criteria
	RS.CO-3 Information is shared consistent with response plans
	RS.CO-4 Coordination with stakeholders occurs consistent with response plans
	RS.CO-5 Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

CATEGORY	SUBCATEGORY
Communications (RC.CO) Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTS, and vendors).	**RC.CO-1** Personnel know their roles and order of operations when a response is needed
	RC.CO-2 Reputation is repaired after an incident
	RC.CO-3 Recovery activities are communicated to internal and external stakeholders as well as executive and management teams

(adapted from **nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf** *pages 23, 41–44)*

FIRST CSIRT Services

The FIRST CSIRT Services Framework[4] describes services and functions of incident response teams within a high-level framework in order to assist in a community-wide standardization and the selection and establishment of a team's services portfolio. It is important to note that you are not expected to provide all services, and each team should select its services based upon its mission, constituents, resources and capacity. The structure of the framework is based on four elements: Service Areas, services, functions, and sub-functions.

Communication Services

There are various services within the CSIRT Services Framework that address communications, as they relate to security operations and incident response services. Some of these include Information Security Incident Coordination, Crisis Management Support, Vulnerability Disclosure, Situational Awareness Communication, and Awareness Building, to name a few.

4 **first.org/standards/frameworks/csirts/csirt_services_framework_v2.1**

FIRST CSIRT Services Framework

SERVICE AREA 1
Information Security Event Management
- Monitoring and Detection
- Event Analysis

SERVICE AREA 2
Information Security Incident Management
- Information Security Incident Report Acceptance
- Information Security Incident Analysis
- Artifact and Forensic Evidence Analysis
- Mitigation and Recovery
- **Information Security Incident Coordination**
- **Crisis Management Support**

SERVICE AREA 3
Vulnerability Management
- Vulnerability Discovery/Research
- Vulnerability Report Intake
- Vulnerability Analysis
- Vulnerability Coordination
- **Vulnerability Disclosure**
- Vulnerability Response

SERVICE AREA 4
Situational Awareness
- Data Acquisition
- Analysis and Synthesize
- **Communication**

SERVICE AREA 5
Knowledge Transfer
- **Awareness Building**
- **Training and Education**
- Exercises
- Technical and Policy Advisory

(*Adapted from* **first.org/standards/frameworks/csirts/csirt_services_framework_v2.1**)

The Information Security Incident Coordination service emphasizes the need for efficient and effective communications with stakeholders and constituents. Media Communication is a function of this service, and engagement with the media may provide accurate and timely information about ongoing events and incidents in order to avoid rumors or misleading information. Relationships with the media will be discussed in the next section, as part of communications responsibilities of information security incident management. The Crisis Management Support Service will be addressed in the subsequent section and address communications responsibilities of crisis management support.

Communications Responsibilities: Information Security Incident Management

The Information Security Incident Management Service Area includes the incident coordination service, among others. This service emphasizes the need for efficient and effective communications with stakeholders and constituents regarding preventing or responding to cybersecurity incidents. Media Communication is also function of this service, and engagement with the media may provide accurate and timely information about ongoing events and incidents in order to avoid rumors or misleading information.

Communications with the general public and/or constituency, as well as relationships with the media, will be discussed in detail in the following sections. It is important to understand and remember that in certain circumstances, the media can assist in the coordination and mitigation of incident response.

Communications with the General Public and/or Constituency

Sharing information and communicating with the general public and/or your constituency is appropriate in many different scenarios. These can range from proactive communications to reactive communications. Examples include, but are not limited to, the following:

- general security awareness and education
- advertised list of services for constituency
- compliance with reporting requirements
- notification of extremely dangerous or wide spread attacks
- notification of new threats and risks
- notification of mitigations
- helping people prevent exposure

Each scenario may be unique, and careful consideration should be given to when to release information to the public and what information should be released.

Ask the following questions when determining when to release information.

- *Does this affect them?*
- *Is there urgency or severity?*
- *What is the major problem (high-level description)?*
- *How will the public react?*
- *Does the organization have the capacity to respond to inquiries from the public?*

Consider the following types of information when determining what information to release.

- new vulnerabilities
- current intruder activity
- current and potential threats
- technical or procedural documentation (mitigation strategies, for example)
- best practices
- trends and statistics

Each document you publish will be unique, but it is generally the case that the information published falls into a small number of categories. Most commonly, you may publish information about new vulnerabilities or intruder activity that is relevant to your constituents. Organizations may also publish information that provides technical background or best practice information. It will be helpful for your organization if you identify what type of information you will publish before you begin publishing anything, either proactively or reactively.

Organizations should also consider different methods and mechanisms for publication, depending on the severity and urgency of the information, as well as the audience.

- Think about the mechanisms for broadcasting or publishing materials.
- Certain methods of publication may be used over others depending on the timeframe for getting information released.
- Determine whether the target audience needs to access the information or read it on mobile devices, email, etc.

Below are some examples of communications mechanisms.

Communications Mechanisms

PUBLICATIONS	Whitepapers/reports	Webinars
	Research papers	Podcasts
	Blogs	News stories
ALERTS AND WARNING	Emails	Web pages
	Texts	Social media
OUTREACH	Speaking engagements	Conferences
	Presentations	Training
	Social media	Other publication types (blogs/webinars/ podcasts)

Identifying different document types of information sharing templates before you have the need for them will be important in proactively managing an incident. This will also help prepare staff for all of the different scenarios that you may encounter, and determine the appropriate audience and level of review required for each publication.

Ensure that each of these document types has

- a purpose
- a basic structure
- means of (and schedule for) distribution
- quality assurance procedures
- an identification scheme (discrete number and/or ID)

Quality assurance and review is also extremely important when releasing information to the public or your constituency. Content should be reviewed for accuracy, clarity, and appropriate audience.

TRUST TIP

The quality and timeliness of the information released will help establish and build trust with your constituency!

Content for Specific Communications: Vulnerabilities, Threats, and Incidents

This section includes information specific to communications regarding different types of events: vulnerabilities, threats, and incidents. Your constituents or the media may have different types of questions depending on the event, so it is best to be prepare responses to all possible questions related to the vulnerability, threat, or incident that you may be handling.

FOR ALL EVENTS

- ☐ Consider whether the information is:
  - Relevant
  - Timely
  - Accurate
- ☐ Does the information have any classification system applied to it?
  - Traffic Light Protocol (TLP)
  - Government classification systems
  - Intra-organizational restrictions
- ☐ Are different communications templates required?

ALWAYS PROVIDE

- ☐ Source information
- ☐ Applicable groups, technologies, or processes that are affected.

Vulnerabilities

- ☐ What systems and/or configurations are vulnerable?
- ☐ Does a patch exist?
- ☐ Mitigation instructions
  - Do automated mitigation methods exist?
  - What level of effort is required to mitigate?
  - How long will automated or manual mitigation methods take?
  - What tools or technologies are required to implement mitigation method(s)?
- ☐ Effects on unpatched systems
- ☐ Level of access granted by vulnerability
- ☐ What group discovered it?
- ☐ What identifiers exist (CVE, etc.)?
- ☐ Describe prevalence of vulnerability among constituency, if able.

Threats

- ☐ Have threat actors been identified?
- ☐ What is the profile of technologies, processes, or people targeted by threat actors?
- ☐ What, if any, blacklists are effective against threat actors?

Incidents

- ☐ Is the incident ongoing?
- ☐ How long has the incident been in progress?
- ☐ When were indicators of the incident detected?
- ☐ What happened and what is the result of the incident?
- ☐ Is there a mitigation?

Media Management Guidance

Media management is a key component of communications planning. You should carefully consider strategies and plans pertaining to managing and communication with the media. It is important to remember that the news does not wait for you to be prepared. Computer security problems threaten economies and as a result affect people's lives in one way or another. Incident response work is newsworthy, and the financial stakes and risks only continue to increase with the passage of time. While the media may not be considered your organization or team's constituency or customer, *it is more than likely that constituencies and customers are receiving information from the media, thus increasing the importance of a strategy to specifically address the media.*

Policies and procedures must be in place for responding appropriately to the media's need for information. While it's important to develop a tailored media strategy to manage the media in the event of an incident, there are some general guidelines that can help develop effective strategies.

First, you should understand the needs of the media and your organization before designing a strategy for media management. It is not only important for organizations to develop a media management strategy for incident management communications, but you must also consider how to do the following:

- Use the media to help disseminate important information quickly when needed.
- Maximize the value of the time spent by technical staff members interacting with media.
- Educate the public about cybersecurity issues and network survivability.
- Increase recognition of your organization among audiences that are essential to the its success.

The media need security groups or experts to

- generate stories about specific security problems or incidents.
- explain the risks and technologies involved.

Security teams and organizations need the media to

- raise awareness and educate the public.
- inform the community, policy makers, and the general public about specific problems and solutions.
- help establish public name recognition for CSIRT services.

Media Management Considerations

It is important that you understand media goals and how your own goals either align with or are contrary to the media's goals. In any case, it is important to provide timely and accurate information. To counter speculation and rumors, you must determine what can be said or what is known versus what should not be disclosed or what is unknown at the time.

Media goals will be different, depending on the type and source of media. These goals may include the following:

- sharing as much information as possible, including speculation
- obtaining leads and site confirmation from a CSIRT
- confirming rumors
- gaining readership or subscribers

Your organizational or team goals may be to do the following:

- assist affected sites and organizations
- communicate problems and solutions to the community
- maintain confidentiality
- maintain the trustworthiness of your organization/team

You should anticipate media interest and work to develop a standard set of frequently asked questions (FAQs), so that your team has materials ready to provide to media outlets when required. A checklist or standard template should also be provided internally so that every individual on the team is aware of the appropriate responses to media requests and/or on-duty personnel are equipped with proper information and training on media management. Ultimately, the media may rely on your organization or team to be the cybersecurity subject matter expert (SME), so be prepared to offer information to an audience of varying skillsets and expertise.

While you would provide or use these materials in a reactive scenario, there are also proactive steps that organizations can take before a crisis occurs. When possible, organizations should consider methods and mechanisms to provide information proactively to media outlets. These proactive measures might include fact sheets, discussions, or even training; proactive measures aid in relationship building with the media, and contribute to the messaging and reputation of an organization. They may also mitigate confusion or misleading information from the onset of an incident or a crisis.

While the motives and objectives of media outlets may be counter to your organization or team's goals, remember that the media may also be an important ally. The media helps spread information; it is a mechanism to get your message to constituents. Consider leveraging an established relationship with the media, or attempting to develop those relationships.

TRUST TIP

Remember—the way you handle the media in a crisis will ultimately affect the level of trust your constituencies place in you!

How to Influence the Story

Here are some tips to help support the story and aid in your narrative of an event or incident:

- **Keep it simple.**
- **Use technical language that is appropriate for the audience and technical sophistication of the writer or interviewer.**
- **Do not assume the reporter knows anything.**
- **Know the story you want to tell.**
- **Determine your key objectives.**
- **Define 2–3 key messages you want to convey.**
- **Repeat your key messages frequently.**
- **Remember, there is no such thing as "off the record."**

If resources and funding allow, the hiring and designation of media relations staff is a best practice for media management. Media or public relations staff can help protect your organization and its staff by

- including all media requests
- establishing relationships with media organizations who have good track records
- deciding which media requests warrant a response
- setting expectations and ground rules for interactions between media and CSIRT staff
- training staff on media communications and best practices
- providing background information on the organization and its functions to media representatives

Media Question Examples

The following questions are examples of potential media questions that your organization may encounter. Use these questions to build templates or preemptively develop FAQ materials for both your constituency and the media. While the answers to the questions may be highly situationally dependent, designated staff should, at the very least, be prepared to answer these common questions. Staff should practice handling example media questions as part of ongoing training and preparation.

- ☐ How serious is the threat?
- ☐ How much damage can be done?
- ☐ Is it global/national in scope?
- ☐ What systems are vulnerable or affected?
- ☐ Who is affected?
- ☐ How can you prevent it?
- ☐ How does it work?
- ☐ How can you fix it?
- ☐ How many reports have been received?
- ☐ How much damage has been reported?
- ☐ How does it compare to other attacks?
- ☐ What is the estimated cost of the activity?
- ☐ How fast is it spreading or how wide-spread is the activity?
- ☐ Can the attacker be traced?
- ☐ Where was it first reported from?
- ☐ What software or OS versions are vulnerable or affected?
- ☐ Where do I go for help?
- ☐ How do I report the activity or vulnerable systems?
- ☐ What resources are available?

Communications Responsibilities: Crisis Management Support

When you develop a crisis communications plan or support service, use the CSIRT Services Framework to help your organization set goals, understand desired outcomes, and implement planning.

The purpose of the Crisis Management Support Service is to "provide expertise and contacts to other security experts, CSIRTs, and CSIRT communities in order to help mitigate the crisis."[5] There is a potential for information security incidents to cause or contribute to an organizational or national crisis. In this case, incident response teams will apply their expertise and resources in managing the crisis, establishing communication services, and providing points of contact throughout the crisis. The Crisis Management Support service, as defined by the FIRST CSIRT Services Framework, should have the following functions:

- information distribution to constituents
- information security status reporting
- strategic decision communications

These particular functions provide communications resources and access to accurate and timely information that will lend to informed, strategic decisions. You must distribute information to constituents to maintain trust-based relationships. The effects of the incident must be clearly communicated with stakeholders and constituents. How, what, and when to communicate information must be decided (preferably in advance of a crisis).

Major Incident Handling and Crisis Management

Before discussing crisis communications further, you need to understand what constitutes "major incident" handling and "crisis" management. Each country, economy, or organization may determine what criteria meet the definition of a crisis. For some industries or countries, this may be determined by regulatory requirements.

For example, in the United States, the Federal Information Security Modernization Act (FISMA) defines the criteria for both major incidents and breaches that constitute major incidents. In the event of a major incident, there are congressional and U.S. Cybersecurity and Infrastructure Security Agency (CISA) notification requirements, among other additional reporting requirements. Agencies address these criteria within Business Continuity, Continuity of Operations, Incident Response, and Breach Response plans; however, recognizing the importance of communications during a major incident or cybersecurity crisis is critical—thus the growing need for a crisis communications plan.

You can expect crisis communications to be somewhat different than routine communications. There may be additional organizational plans that a crisis communication plan is linked to or aligned with, roles and responsibilities may shift in the event of a crisis, and communication with stakeholders may be more frequent due to the severity of the situation. Where the crisis communications plan is housed, as well as how it is incorporated into other organizational plans, largely depends on your individual organization. What is important to recognize is the need to proactively plan for crisis communications unique to cybersecurity crises (major incidents, breaches, cyberattacks, etc.), as cybersecurity crises may be responded to differently than other types of crises (natural disasters, for example). For more on types of organizational plans and the corresponding purpose, scope, and relationship to other plans, as detailed in NIST SP 800-34, see Appendix A.

Recommended Procedures for Handling Major Incident Communications

This list is a quick reference guide of recommended high-level procedures for the handling of major incidents, as they relate to your ability to both manage the incident and communicate with your constituents and stakeholders. Overall crisis management planning is outside of the scope of this document, but the checklist below provides pointers specifically for the communications aspect of crisis management.

CREATE STANDARD PLANS AND PROCEDURES THAT CAN BE FOLLOWED WHEN SUCH ACTIVITY OCCURS	Identify a prioritization process of what should be done first.
	Create a manual of instructions to be followed during periods when handling major event incidents.
	Identify standard information guidelines and recovery strategies that can be released for certain types of activity while analysis of the ongoing incident is occurring.
	Create templates that can be used for advisories, FAQs, and technical documents.
	Identify processes for obtaining and assigning backup staff.
	Train backup staff ahead of time.
	Make arrangements in advance for secure communication mechanisms with third parties such as law enforcement, other CSIRTS, vendors, and constituents (e.g., PGP, digital certificates, etc.)

5 **first.org/standards/frameworks/csirts/csirt_services_framework_v2.1**

CREATE A SPECIAL TEAM WITH PRIORITIZED ASSIGNMENTS	Identify and/or assign a lead for the priority incident.
	Stagger staff to cover out of hours and business hours.
	Focus technical staff on analysis and information gathering versus answering individual calls.
CREATE INSTRUCTIONS FOR STAFF	Describe current status and any special reporting procedures.
	Identify analysis and response questions that need answered.
	Create special tools or procedures for staff specific to ongoing activity.
INCREASE COVERAGE OF HOTLINE OR HELP DESK PHONE	Identify staff to handle calls from high profile sites.
	Detail speaking points—what can be said and what not to say.
	Detail special information to capture from or provide to callers.
	Give out pointers to available resources.
PROVIDE INITIAL RESOURCES FOR CALLERS AND REPORTERS	Create a recorded message that can be updated.
	Place current knowledge or status on a Web page; update this as more information is made available.
	Create an FAQ for all incoming questions. Send it to all callers and reporting sites.
	Publish known statistics, scope, and FAQs on a Web page.
PROVIDE INITIAL RESOURCES FOR MEDIA	Create talking points for staff when speaking with media.
	Hold a press conference or issue a press release when appropriate for maximum exposure.
	Set up media hotlines or recorded messages.
	Keep your staff and management updated!
	Have one person assigned to keep management updated.
	Use intranets, email, or internal recorded phone messages to keep staff up to date.

Crisis Communications Resources

The following documents and resources supplement your efforts to build and implement communication plans and crisis management plans within your own organizations.

NIST SP 800-184: *Guide for Cybersecurity Event Recovery*

nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf

NIST SP 800-34 rev 1: *Contingency Planning Guide for Federal Systems*

nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

GovInfoSecurity

govinfosecurity.com/nists-7-step-contingency-planning-process-a-2615

Inter-University Consortium for Political and Social Research (ICPSR)

icpsr.umich.edu/icpsrweb/content/datamanagement/disaster/crisis-communications.html

Disaster Recovery Institute (DRI) International

drii.org/resources/professionalpractices/EN

Digital Preservation Management

dpworkshop.org/dpm-eng/workshops/management-tools/disaster-preparedness/communication

Tech Target

searchdisasterrecovery.techtarget.com/Complete-crisis-management-guide-and-free-template

searchdisasterrecovery.techtarget.com/tip/Crisis-management-plan-12-key-elements-for-resilience

searchdisasterrecovery.techtarget.com/tip/Roles-and-responsibilities-of-a-crisis-management-team

searchdisasterrecovery.techtarget.com/definition/crisis-communication?track=NL-1823&ad=933087&src=933087&asrc=EM_NLN_125200785&utm_medium=EM&utm_source=NLN&utm_campaign=20200323_Word%20of%20the%20Day:%20crisis%20communication

Deloitte

deloitte.com/content/dam/Deloitte/no/Documents/risk/cyber-crisis-management.pdf

MIT Technology Review
technologyreview.com/2016/04/20/160885/crisis-communication-after-an-attack/

RSA Conference
rsa.com/en-us/blog/2016-01/incident-response-implement-a-communications-plan

Institute of Electrical and Electronics Engineers (IEEE)
ieeexplore.ieee.org/abstract/document/6542532

OutSecure Inc.
outsecure.com/incident-response-crisis-management/

MindTools
mindtools.com/CommSkll/CommunicationsPlanning.htm

University of Kansas
ctb.ku.edu/en/table-of-contents/participation/promoting-interest/communication-plan/main

Public Speaking Best Practices

Public speaking and presentation skills are important for all incident handlers and security personnel who are expected to communicate with internal and external stakeholders, as well as relay information about incidents to their constituency, community, and/or the media. Public speaking skills are especially important in the event of a crisis or major incident.

There are a many best practices and publicly available research on public speaking and the improvement of communication, presentation, and public speaking skills. In general, you should practice the following to improve your effectiveness as a public speaker:

- **know your audience**
- **determine your key message**
- **engage your audience**
- **use storytelling or narratives**
- **be cognizant of body language**
- **plan and practice**
- **first and last impressions matter**

Resources for Public Speaking—including best practices, blogs, videos, and courses:

Presentation Zen
presentationzen.com/

Coursera
coursera.org

Ted's Secret to Great Public Speaking
ted.com/talks/chris_anderson_ted_s_secret_to_great_public_speaking

Duarte
duarte.com/presentation-skills-resources/

MindTools
mindtools.com/CommSkll/PublicSpeaking.htm

Free Resources

inc.com/larry-kim/nine-places-to-learn-public-speaking-for-free.html

Storytelling Tips

wistia.com/learn/marketing/how-telling-your-best-story-generates-leads-sales-and-lots-of-love

themuse.com/advice/5-sciencebacked-ways-to-give-better-presentations-even-if-you-hate-public-speaking

Speaking with the Media

bu.edu/prsocial/best-practices/public-relations/10-tips-on-speaking-with-the-media%E2%80%8B%E2%80%8B/

Other Tips

firstround.com/review/Powerful-Tips-from-Techs-Top-Media-Trainer-and-Speaking-Coach/

inc.com/brent-gleeson/20-tips-for-mastering-art-of-public-speaking.html

forbes.com/sites/forbesagencycouncil/2020/01/28/10-public-speaking-tips-from-a-pr-expert/#20bfcb863915

Appendix A:
Types of Organizational Plans

There are many different types of organizational plans; communications are often their focal point. Whether you are looking to further develop organizational plans and policies, or want to understand the relationship between the various plans in order to align them across an organization, it is important to determine and understand common terminology, purpose, and scope of each plan.

The National Institute for Standards and Technology (NIST) *Special Publication 800-34 rev 1: Contingency Planning Guide for Federal Systems* provides a summary of various plans that might apply to an organization in the handling of cybersecurity events, incidents, and crises.

An organization may have various types of plans that address communications, business continuity, and disaster or crisis planning. Communications should be documented in each plan—and there may even be a standalone organizational communications plan. Crisis communications plans will ultimately identify both internal and external communication stakeholders, mechanisms, and procedures to be activated in the event of a predefined crisis or major incident. The crisis communications plan could be a part of the BCP, COOP, or Crisis Management Plan. It could be activated as a standalone document by the procedures detailed within a parent plan, or it can be a specific subsection within a larger organizational communications plan. Where the crisis communications plan is housed, as well as how it is incorporated into other organizational plans, largely depends on your individual organization. See the table below for high-level examples of organizational plans.

Types of Organizational Plans

PLAN	PURPOSE	SCOPE	PLAN RELATIONS
BUSINESS CONTINUITY PLAN (BCP)	Provides procedures for sustaining mission/business operations while recovering from a significant disruption.	Addresses mission/business processes at a lower or expanded level from COOP.	Mission/business process focused plan that may be activated in coordination with a COOP plan to sustain non-mission essential functions.
CONTINUITY OF OPERATIONS (COOP) PLAN	Provides procedures and guidance to sustain an organization's essential functions at an alternate site for up to 30 days; mandated by federal directives.	Addresses essential functions at a facility; information systems are addressed based only on their support of the mission essential functions.	Focused on essential functions; may also activate several business unit-level BCPs, ISCPs, or DRPs, as appropriate.
CRISIS COMMUNICATIONS PLAN	Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors.	Addresses communications with personnel and the public; not information system-focused.	Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event.
CRITICAL INFRASTRUCTURE PROTECTION (CIP) PLAN	Provides policies and procedures for protection of national critical infrastructure components, as defined in the National Infrastructure Protection Plan .	Addresses critical infrastructure components that are supported or operated by an agency or organization.	Risk management plan that supports COOP plans for organizations with critical infrastructure and key resource assets.
CYBER INCIDENT RESPONSE PLAN	Provides procedures for mitigating and correcting cyber incidents.	Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information.	Information system-focused plan that may activate an ISCP or DRP, depending on the extent of the incident.
DISASTER RECOVERY PLAN (DRP)	Provides procedures for relocating information systems operations to an alternate location.	Activated after major system disruptions with long-term effects.	Information system-focused plan that activates one or more ISCPs for recovery of individual systems.
INFORMATION SYSTEM CONTINGENCY PLAN (ISCP)	Provides procedures and capabilities for recovering an information system.	Addresses single information system recovery at the current or, if appropriate, alternate location.	Information system-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP, and/or BCP.
OCCUPANT EMERGENCY PLAN (OEP)	Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat.	Focuses on personnel and property particular to the specific facility; not mission/business process or information system-based.	Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation.

Adapted from **nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf** *page 11*

Appendix B: Communications Plan Inclusions

The following are recommended inclusions for a communications plan, whether it be a general organizational communications plan, a standalone crisis communications plan, or a communications section within a larger crisis management plan. This list is not exhaustive; the contents of a communications plan will vary based upon individual organizational needs and audiences. However, the main sections provided below should always be documented. This section highlights key topics for consideration when developing your own communications plan. A crisis communications plan would also incorporate additional information, such as the criteria for when the crisis management plan goes into effect and specifically when to follow the crisis communications plan.

Communications Plan Sample Sections

SECTION	DESCRIPTION
INTRODUCTION/OVERVIEW	Provides a brief summary and general context behind the intent of the communications plan. Other pieces of the introduction may include "Intended Audience" and "Use of the Document."
PURPOSE	Highlights the high-level purpose behind the creation of the plan. It may refer to other authorities, governing directives, or guidance documents, as they relate to communications. It should address the problem—or challenge—that a communications plan addresses or mitigates.
SCOPE	Outlines what is within the scope of the communications plan and who it applies to. If applicable, it can also mention what items may be out of scope. The following two sections may be incorporated into purpose or scope, but should be addressed early on in the communications plan, if applicable.
STRATEGY/VISION	Optional, but may be appropriate as communications procedures should align with overall organizational strategy, mission, and vision.
EXISTING POLICIES AND PROCEDURES	Highlights key authorities and existing policies and procedures that either directly or indirectly affect communications, and how to incorporate or align existing documentation to the communications plan. Establishing a document hierarchy as it relates to existing policies and procedures is helpful. Reference or supporting policies may also be included in an appendix. For crisis communications, this section may specifically identify the criteria for activation of the crisis management or crisis communications plan.
HISTORY/VERSION	Includes historical details such as publish date, document version number, or any applicable cancellation dates. This can be included in a change log at the beginning or end of the plan.
ROLES AND RESPONSIBILITIES	Clarifies organizational roles and responsibilities that support communications. The roles and responsibilities section can address organizational or individual roles. If appropriate, roles and responsibilities can be detailed within an appendix. For crisis communications, this section should specifically address when and how these roles are placed into action.
POINTS OF CONTACT/ CONTACT INFORMATION	Can be provided as an appendix, but it must be clear to the reader who should be contacted, when they should be contacted, and how they should be contacted. This has ties to roles and responsibilities, but should be more explicit in stating roles/positions with appropriate contact information and mechanisms.
INTERNAL COMMUNICATIONS AND ESCALATION	Provides detail on when and how to contact internal stakeholders, who the internal stakeholders are (if not clearly delineated within Contact Information), and what the information escalation process would look like for the particular organization.
EXTERNAL COMMUNICATIONS	Ties in roles and responsibilities and escalation to consider the process for communicating externally (customers/constituents, other similar organizations, cross-sector, etc.). This should clearly define who the external stakeholders are, and when and how to contact them.
MEDIA COMMUNICATIONS AND MANAGEMENT	Addresses how and when to communicate with media outlets and sources, and how to manage the interactions and relationships with the media, including who is authorized to speak to the media and what to do when contacted by the media. This may also include a standard set of questions and answers and/or templates prepared in advance of particular types of events or incidents.
MESSAGE MANAGEMENT	Discusses the importance of messaging in communications, and aids in establishing a common organizational message in the event of a cybersecurity incident, breach, etc.
COMMUNICATION MECHANISMS	Discusses the possible communication mechanisms, and when it would be appropriate or relevant to use specific mechanisms. Depending on the organization, this section could also be addressed throughout internal, external, and media communication sections instead of a standalone topic.

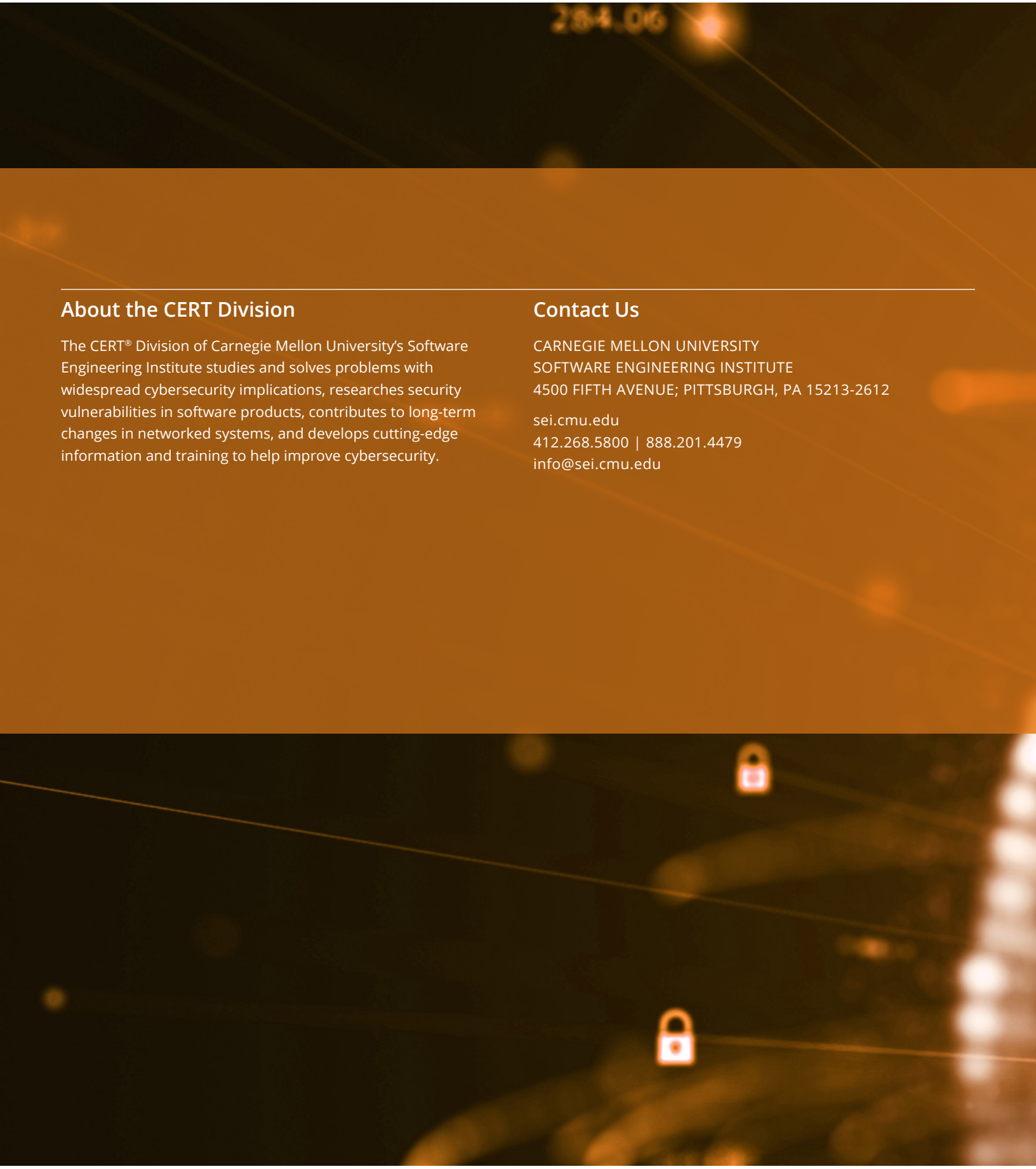
REVIEW/LESSONS LEARNED	Details the organization's policy on review of the communications plan, as well as any other requirements to conduct and document lessons learned as they pertain to communications.
AWARENESS AND TRAINING	Details the organization's policy on awareness and training as it pertains to the communications plan. Examples would include organization-wide awareness training requirements, required training for incident responders or management, etc.
TESTING, AUDIT, AND MAINTENANCE	May be incorporated into lessons learned or awareness and training, however the plan must address how the organization intends to test the plan, preferably on an annual basis at a minimum. This may include table top exercises or drills to simulate a scenario in which the plan is placed into action. An organization should also address how often to review and audit the plan and who is responsible for the ownership and maintenance of the communications plan.
GLOSSARY/TERMINOLOGY	Most likely, there will be a significant amount of terms or acronyms included throughout the plan; a glossary of terms can assist in clarifying any confusion and identifying a common taxonomy for the reader.
APPENDICES	Appendices are a good way to include content without detracting from the flow or brevity of the plan. If there are templates, lists, terms, etc. that can be further detailed in an appendix, they may be referenced and linked appropriately within the plan. Appendices may include, but are not limited to the following: • Templates • Organizational charts • Process/Communications workflows • Comprehensive listing of communications mechanisms • Frequently Asked Questions (FAQs)

Your feedback is welcome.

If you have feedback you'd like to give on this publication, we would love to hear it. Please send an email to **security-operations@cert.org**

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM20-1144



About the CERT Division

The CERT® Division of Carnegie Mellon University's Software Engineering Institute studies and solves problems with widespread cybersecurity implications, researches security vulnerabilities in software products, contributes to long-term changes in networked systems, and develops cutting-edge information and training to help improve cybersecurity.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu