**Name of Organization**

**Incident Response, Customer &**

**Media Communication**

December 2021

**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

The (Name of Organization) Customer and Media Communication Document is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. This document is unclassified but contains sensitive information.

**Table of Contents**

[I. Introduction and Purpose 4](#_Toc88584422)

[II. Training 5](#_Toc88584423)

[III. Coordination and Collaboration 5](#_Toc88584424)

[IV. Integrating with Federal Support 6](#_Toc88584425)

[Information Distribution 6](#_Toc88584426)

[Notification Letter and Email 7](#_Toc88584427)

[V. Public Media 7](#_Toc88584428)

[Media and Press Release Notification 7](#_Toc88584429)

[VI. Customer Letter/Email Template 13](#_Toc88584430)

[Table 1: Customer & Media Communication Matrix 14](#_Toc88584431)

# Introduction and Purpose

This document defines requirements for establishing specific Customer and Media Communication Notifications in the event of an incident and is aligned with *National Incident Management System (NIMS) Basic Guidance for Public Information Officers*. The purpose for establishing Customer and Media Communication Notification Requirements is to appropriately report on a data incident and the impact the incident has on the availability, confidentiality, and integrity of organizational data and potential impact on associated customers and vendors. Furthermore, to address the organization’s responsibilities pertaining to press releases, drafting of notification documents, and organizational communications with customers and vendors.

Public information efforts, which should begin well in advance of an incident or planned event, can involve a combination of planning, resource gathering, organizing, training, and exercises.

Public information planning allows Public Information Officers (PIO)s to coordinate and communicate lifesaving measures — such as evacuation routes, alert systems, and other public safety information — to diverse audiences in a proactive, timely, and consistent manner. Community risk reduction and other public education efforts help prepare citizens/employees to mitigate or respond to a variety of events. For detailed operational practices to help PIOs perform their duties within the National Incident Management System (NIMS) Command and Coordination structures please review document *National Incident Management System Basic Guidance for Public Information Officers.*

# Training

The Federal Emergency Management Agency (FEMA) encourages PIOs to participate in ongoing emergency management training. This includes basic public information courses; Incident Command Systems (ICS) courses; and training in social media content, listening and engagement, conducting interviews, writing (including nontraditional media, talking points, and media releases), and understanding the role of a Joint Information Center (JIC). Prerequisite and Prerequisite and recommended courses are available through the Emergency Management Institute (EMI).

# Coordination and Collaboration

At all levels of incident management, public information personnel are responsible for gathering, analyzing, and proactively disseminating information to ensure accurate, timely updates on the incident or event. The Incident Command System (ICS) integrates facilities, equipment, personnel, procedures, and communications into a common organizational structure. ICS applies to a variety of incidents, organizations, and government entities at all levels and where applicable communication and coordination should be aligned with ICS especially when incidents involve different agencies and where multiple PIOs are collaborating. In those cases, the Incident Commander (IC) or Unified Command designates one person as the lead PIO. All PIOs work in a unified manner, speaking with one voice and ensuring consistent messaging. The IC, in collaboration with the lead PIO, approves the release of incident-related information. In incidents involving multiple agencies, leadership may establish a Joint Information Center (JIC). The PIO participates in or leads the JIC.

For these incidents specific communication Protocols have been established:

* National Incident Communications Conference Line (NICCL)
* State Incident Communications Conference Line (SICCL)
* Private Sector Incident Communications Conference Line (PICCL)

More detailed information can be found on [FEMA National Response Framework](https://www.fema.gov/emergency-managers/national-preparedness/frameworks/response) and Emergency [Management Assistance Compact (EMAC)](https://www.emacweb.org/).

# Integrating with Federal Support

Incidents – depending and size and criticality – may be managed at the organizational level, where the organization retains their independence and manages the incident by themselves. For larger incidents that impact multiple agencies, or regions, or a part of a national emergency or incidents may require joint collaboration which will include federal support. In these cases, Incident Management organizations retain their independence while collaborating through the JIC to generate common public information. Incident command, Emergency Operations Center (EOC) leadership, or Multiagency Cooperation Group (MAC) Group members may be responsible for establishing and overseeing JICs, including the processes for coordinating and approving public communications.

Federal support follows the standard operating procedures of Emergency Support Function (ESF) #15—External Affairs. ESF #15 integrates and coordinates the functional areas of public affairs; community relations; local, state, tribal, and territorial affairs; the private sector; and congressional affairs. Primary leaders for ESF #15 include staff from the U.S. Department of Homeland Security (DHS) and FEMA, as well as staff from other Federal agencies in specific response scenarios. DHS/FEMA encourages local, state, tribal, and territorial entities to work in partnership to ensure the effective, efficient production and dissemination of emergency information. DHS encourages entity PIOs to co-locate within the incident JIC to facilitate coordination, cooperation, and unified messaging.

## Information Distribution

The classification of all information at the time of an incident is to be considered confidential, and at no time should any information be discussed with anyone outside of the organization without approval of the Incident Commander, executive management, and/or company legal counsel.

Public or media statements must be carefully managed to ensure that any investigation/legal proceedings are not jeopardized in the future, and reputational damage is minimized. Decisions concerning the disclosure and method of disclosure of incident information will only be made by a designated spokesperson assigned by the Cybersecurity Incident Response Team (CIRT), likely someone from the Communications Team or a representative coached by the Communications Team.

Inquiries from media agencies must be channeled to the designated CIRT representative. Employees found to be discussing any aspects of incidents without approval from executive management/legal counsel will be subject to disciplinary action, up to and including termination of employment.

## Notification Letter and Email

Do not disclose anything that hampers the investigation, gives additional information to those who would do harm, etc., or might impact future legal proceedings. Release information only through (Organizational) approved channels. The Notification Letter and Email should contain the following:

* Summary of what happened
* Timescales of breach - When the breach occurred and/or when was it detected
* How it was detected
* What data was potentially compromised?
* How much data was compromised?
* Impacted Persons and the Information at Risk
* Reason for this notification
* What steps are/were being taken
* Is any data known to be fraudulently used or is notification precautionary?
* What steps should individuals take, if any
* Apology, expression of regret, or statement
* Anticipated next steps, if any.
* Who to contact for additional information?
* Signature

# Public Media

## Media and Press Release Notification

Prior to disclosure of Organizational incident information to the public or media, communication should be approved by the appropriate Organizational personnel, starting with the Incident Commander and/or designate. Furthermore, ONLY the appointed and approved Organizational Representative should deliver such information. The following questions can be used to guide with interactions with the media, and providing a press release:

* Do I need to issue a press release?
* Who will the press release be sent to? Victims? Media outlets?
* What medium will be used for the press release?
* Do I have legal obligations relative to the press release? Is it serving as "substitute notice" per state law?
* The Press Release Summary Statement should contain a summary of the entire story so that those reading the release know exactly what is happening.
	+ What are you doing?
	+ What type of breach are you announcing? A theft of data?
	+ What is the status? Analysis in progress, case resolved?
* Brief incident details:
	+ Who is affected/not affected?
	+ What specific types of data and/or personal information are involved?
	+ What does evidence suggest so far? For example, no evidence to indicate data has been misused.
* Expression of regret (if appropriate)
	+ If details of the incident are still unclear, it may not be appropriate or advisable to express regret as this may have implications around liability.
* Indicate the steps being taken to prevent this from happening again.
* Major (re)actions taken.
* For more information, please contact Organizational Representative name

Media and Press Release Notification Guidelines

Below are sample statements to use if members of the media call before a press release is issued. All communications with the media should be directed to the Incident Commander or other representative designated by Executive Management. Getting the facts correct is a priority. Do not give information to the media before confirming facts with internal personnel and management. No conjecture, speculation or guesses. Changing information after it is released can lead to media confusion and loss of focus on the key messages.

Pre-scripted Immediate Responses to Media Inquiries

Use this template if the media is “at your door” and you need time to assemble the facts for the initial press release statement. Getting the facts together is a priority. It is important that you do not give in to pressure to confirm details or release information before you have confirmation.

The following responses give you the necessary time to collect the facts.

Pre-scripted Responses

**If on the phone to the media:**

* “We’ve just learned about the [situation, incident, event] and are trying to get more complete information now. How can I reach you when I have more information?”
* “All our efforts are directed at [bringing the situation under control]. I’m not going to speculate about [the situation]. How can I reach you when I have more information?”
* “I’m not the authority on this subject. Let me have [name] call you right back.”
* “We’re preparing a statement now. Can I get back to you in about [number of minutes or hours]?”
* “You may check our website for background information, and I will fax/e-mail you with the time of our next update.”

**If in person at the incident site or in front of a press meeting:**

* This is an evolving [situation, incident, event], and I know you want as much information as possible right now. While we work to get your questions answered, I want to tell you what we can confirm right now:
* At approximately [time], a [brief description of what happened].
* At this point, we do not know [how long the advisory will last, how many customers are affected, etc.].
* We have a [system, plan, procedure, operation] in place. We are being assisted by [local officials, experts, our legal team] as part of that plan.
* The situation is [under, not yet under] control. We are working with [local, state, federal] authorities to [correct this situation, determine how this happened].
* We will continue to gather information and release it to you as soon as possible. I will be back to you within [amount of time in minutes or hours] to give you an update. As soon as we have confirmed information, it will be provided.
* We ask for your patience as we respond to this [situation, incident, event].

Statement Writing Tips

The following information/tips can be used to create a good media statement. Not all of them need to be included, but typically two or three will ensure an effective statement.

**Honesty**

If investigation results clearly point to the organization being at fault, admit it and apologize sincerely. By attempting to deflect responsibility, journalists and the public will be far less forgiving when the details around the incident are exposed and the organization is found guilty.

If the organization is not at fault, this needs to be stated very clearly but without overtly blaming any other individual or organization.

* Words to use: take or share responsibility, committed to openness, transparent.
* Words not to use: blame, fault.

**Context**

Presenting negatives in a broader context can go a long way to minimizing the impact of the bad news. For example, if the story is about a service user who has had a bad experience, you can refer to the many other service users who have had good experiences. This is where external advocates are useful – particularly other service users.

Broadening context also means isolating the incident – simply a case of stating that the negative incident is ‘very rare’/’isolated’ and placing it within a wider, more positive framework.

* Words to use: very rare, isolated.
* Words not to use: frequent mistakes, another error.

**Framing Effect**

The Framing Effect is a form of cognitive bias, which causes people to prefer positive sounding statements over negative ones, despite otherwise being logically identical. Be aware of this form of cognitive bias when developing and delivering messages to the public.

**Partnership**

There are occasions when it is useful to subtly remind a critical audience that you are not solely responsible for the conduct of a particular individual. This can be achieved without it appearing as if you are ‘buck- passing’ or absolving yourselves of responsibility and without upsetting relations with other key partners.

For example, you may simply state that “as one of a number of organizations involved in supporting the individual concerned, you are ‘committed to providing the best possible service for service users in the area’”.

* Words to use: working together, joint responsibility, as one of a number of organizations.
* Words not to use: X is to blame

**Action**

Media statements should not merely talk about the problem; they should stress action on the part of the organization.

You will not improve any media situation if you are seen to be passive in the case of a negative situation or media crisis.

A word of caution: avoid saying you will be holding an ‘investigation’/’inquiry’ in the case. These words are headline-fodder for the media and can imply guilt.

Words to use: taking immediate action, taking appropriate measures, working closely with agencies, law enforcement, other affected parties.

Words not to use: we are holding an investigation; we will look into it.

**Positives**

Don’t be afraid to point out how successful your organization is in any media statement. Mistakes happen and emphasizing the positive things you’ve done can help people see past minor blips.

* Words to use: we have seen positive results, we have been successful in, we will continue to provide the best service
* Words not to use: there are a number of areas we need to work on (unless you accompany that with a positive statement e.g., that you will be taking measures to change this).

**Empathy**

Negative media situations can create a gap between you and the people impacted, be they customers, employees, or the general public. Expressions of empathy can help bridge the gap.

* Words to use: we understand, we appreciate, we know, we recognize.
* Words not to use: these things happen, everyone faces these issues.

**Be Concise**

Journalists are typically not interested in lengthy statements – they would prefer to spend the effort on details of the event/incident. Further, if the person speaking with the media is not accustomed to doing so, lengthy statements may result in the speaker making an error.

As a rule, statements for printed media should be no more than two paragraphs long – one tight sentence per paragraph.

Broadcast media may give you more space, but you should still bear length in mind as the producer/editor may be looking to produce a shortened version of your statement to drop into a later news bulletin.

**Statements**

* Avoid confrontation - the objective of media statements in a crisis is to diffuse the situation – not make it worse. Avoid blaming/buck-passing because it will simply result in a media-based argument between opposing parties – remember journalists love confrontational stories. e.g., ‘They were wrong’, ‘it is not our fault’, etc.
* Avoid ambiguity - weak, ambiguous statements have no place in handling negative media situations and can leave room for the journalist to re-interpret your response. Be robust and clear at all times. Use strong positive words e.g., ‘we are committed to X and will not tolerate Y’. Make sure your statement is completely unambiguous.
* Use personal pronouns - try and avoid referring to your organization by name in your media statement as doing this could reinforce the link between your organization and the negative issue concerned. You may simply use the first-person plural (‘we’/’us’). This also has the advantage of adding a slightly personal and less bureaucratic feel to the statement.

# Customer Letter/Email Template

Credit Card Breach example:

Dear Valued Customer,

As you may be aware, we have announced that we have experienced a criminal intrusion into a portion of our computer network in some of our locations (retail stores, etc.). This criminal intrusion may have resulted in the theft of information including account numbers, card expiration dates, and other numerical information and/or the cardholder’s name. We have not determined that any such cardholder data was in fact stolen by the intruder, and it has no evidence of any misuse of such data.

We are providing this notice out of an abundance of caution to all of our customers who have provided their contact information to the company, including you. YOUR INFORMATION IS NOT NECESSARILY AFFECTED.

(Organizational) believes that the potentially impacted systems were breached during the period of <insert date> through <insert date>.

Upon recognition of the intrusion, we took immediate steps to secure the affected part of our network. An investigation supported by third-party data forensics experts is ongoing to understand the nature and scope of the incident.

We believe the intrusion has been contained and is confident that its customers can safely use their credit and debit cards in our premises/stores. (Organizational) currently has no reason to believe that additional information beyond that described above was stolen by the intruder. However, given the continuing nature of this investigation, it is possible that time frames, location, and/or at-risk data in addition to those described above will be identified in the future.

We have notified federal law enforcement authorities and are cooperating in their efforts to investigate this intrusion and identify those responsible. The press release and this letter have not been delayed as a result of this law enforcement investigation. We have also notified the major payment card brands and are cooperating in their investigation of the intrusion.

We have established a call center to answer customer questions about the intrusion and the identity protection services being offered. The call center will be staffed Monday through Friday 8am-8pm CST and the number to call is:

You are a truly valued customer, and we regret any inconvenience that this may cause you.

Sincerely,

<insert name and title>

## Table 1: Customer & Media Communication Matrix

The following matrix provides a guideline that highlights the responsibility and frequency for communicating status and decisions during the response to an incident.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Personnel  | VP | Senior Leadership | Response Mgmt. | Extended Support BALs, Legal, Partners | Directors | Business Units | Media | Enterprise |
| Incident Commander | P / B |   | A /  B,V,E | P /B,V,E | P /V,E |   |   |   |
| CIRT |   |   | P /B,V,E | A /B,V,E | A /V,E | A /B,V,E  |   |   |
| Communications |   |   |   |   |   |   | P / B,V,E |   |
| IT Management/CTO/CEO/CISO |   | P / B,V,E |   |   |   | P /B,V,E |   | P / B,V,E |

|  |  |  |
| --- | --- | --- |
| Responsibility | Type |  |
| P   = Primary ResponsibilityA = Alternate Responsibility | B   = BriefingC  = Case MessageE   = EmailF   = Fetch MessageV  = Voice Mail | Communication frequency shall be established based on the nature of the incident and SLAs. |