CSR C

Communications Security, Reliability and Interoperability Council

March 2016 WORKING GROUP 2

Emergency Alerting Platforms

WEA Security Sub-Working Group

Final Report – WEA Security

Table of Contents

1 Results in Brief 6

1.1 Executive Summary 6

2 Introduction 8

2.1 CSRIC Structure 8

2.2 Working Group 2 Team Members 9

3 Objective, Scope, and Methodology 10

3.1 Objective 10

3.2 Scope 10

3.3 References and Definitions 10

3.3.1 References 10

3.3.2 Definitions 11

4 Background 12

4.1 WEA Decomposition 12

4.2 Potential Security Risks 13

4.2.1 Risk 1: Insider Sends False Alerts 13

4.2.2 Risk 2: Inherited Replay Attack 14

4.2.3 Risk 3: Malicious Code in the Supply Chain 15

4.2.4 Risk 4: Denial of Service 16

4.2.5 Risk 5: Outsider Sends False WEA Alerts 16

4.2.6 Risk 6: Insider Blocks Real WEA Alerts 16

4.2.7 Risk 7: Outsider Blocks Real WEA Alerts 16

4.2.8 Risk 8: CMSP Infrastructure Testing System Access 17

4.2.9 Risk 9: Security Vulnerability in Existing Standards 17

4.3 Risk-Based Analysis 18

4.4 Security Analysis of the Elements in WEA Chain 18

4.4.1 Alert Originators 18

4.4.1.1 People 18

4.4.1.2 Process 19

4.4.1.3 Software 19

4.4.1.4 Malicious Warning App 20

4.4.2 IPAWS 20

4.4.2.1 IPAWS Message Validation 21

4.4.2.2 IPAWS Alert Originator Access Process 21

4.4.2.3 IPAWS Software Code Base 22

4.4.2.4 IPAWS Logical Connectivity 23

4.4.2.5 Blocking of Valid WEA Messages 23

4.4.3 CMSPs 23

4.4.3.1 Blocking of Valid WEA Messages 23

4.4.3.2 Risks of false base station transmitting a false WEA alert 24

4.4.3.3 Inclusion of URLs and phone numbers used for DOS attacks 24

4.4.3.4 Risk of injecting false WEA alerts into operator equipment 24

4.4.3.5 Risk of injecting malicious software into a CMSP WEA component 25

4.4.4 Alert Recipients 25

4.4.4.1 Malicious Warning App 25

4.4.5 PBS WARN 25

4.4.5.1 Background 25

4.4.5.2 The importance of PBS WARN to WEA Cybersecurity 26

4.4.5.3 Diversity 26

4.4.5.4 Availability 27

4.4.5.5 How Does a CMSP Utilize WARN as a Backup? 27

5 Findings and Recommendations 28

5.1 Findings 28

5.2 Recommendations 29

6 Conclusions 30

Appendix A: Acronyms 31

Appendix B: Glossary 33

Appendix C: Sample MOA – Between FEMA & Alert Originators 35

List of Figures

[Figure 1 - The Four Elements of the WEA Pipeline 12](file:///C:\Users\fkhatibi\Documents\CSRIC\CSRIC%20V\CSRIC%20Emergency%20Alerting%20Platform%20Security%20Final.docx#_Toc444669484)

[Figure 2 – Message Validation 21](#_Toc444669485)

[Figure 3 - PBS WARN Redundancy 28](#_Toc444669486)

List of Tables

[Table 1 - Working Group Structure 8](#_Toc444669487)

[Table 2 - List of Working Group Members 9](#_Toc444669488)

# Results in Brief

## Executive Summary

The Wireless Emergency Alerts (WEA) service is a collaborative partnership that includes the cellular industry, Federal Communications Commission, Federal Emergency Management Agency (FEMA), and U.S. Department of Homeland Security Science and Technology Directorate. Like other cyber-enabled services, WEA may be subject to cyber threats that may prevent its use or damage the credibility of the service it provides.

The objective of the Security SWG of CSRIC V WG2 was to review current standards-defined and deployed Wireless Emergency Alert (WEA) security practices and recommend actions. The review covered end-to-end security aspects of WEA including the integrity of all interfaces, insuring the integrity of the WEA message as it transverses from the alert originators and across the carrier networks, and security of message data on handsets. Consideration was given to new technologies and cyber risks to WEA. The working group used an analysis technique developed by researchers at the Software Engineering Institute for evaluating and addressing these possible risks.

The following risk scenarios were identified in a study of CMSPs conducted by the Software Engineering Institute and funded by DHS, as well as other sources:

* Risk 1: Insider Sends False Alerts
* Risk 2: Inherited Replay Attack
* Risk 3: Malicious Code in the Supply Chain
* Risk 4: Denial of Service
* Risk 5: Outsider Sends False WEA Alerts
* Risk 6: Insider Blocks Real WEA Alerts
* Risk 7: Outsider Blocks Real WEA Alerts
* Risk 8: CMSP Infrastructure Testing System Access
* Risk 9: Security Vulnerability in Existing Standards

Each potential risk was analyzed based on key criteria:

* Probability
* Impact
* Risk exposure

For Alert Originator’s access to their alerting software, the FEMA Memorandum of Agreement (MOA) and Rules of Behavior require the use of strong passwords and forbid password sharing. A strong password could be all that prevents a bad actor from sending an unauthorized WEA to the entire county, state, or applicable area of responsibility. The digital certificate is quite literally the key required to send an alert. FEMA maintains the chain of custody for handling certificates down to the person(s) authorized in the MOA. From that point it is the Alert Originator’s responsibility to safeguard the digital certificate once they take possession. The Alert Originator should only contract with an alerting software vendor that they trust, because the digital certificate is usually uploaded into the vendor alerting software tools.

The Alert Originator is also responsible for making policy for how their agency will use WEA. The absence of a documented policy creates a condition where access to the alerting software is not controlled or enforced. The agency staff must exercise the policy in a training mode to address questions and concerns that may come up and prepare for timely use in an emergency.

The working group identified the risk of outside actor with malicious intent creating a non-WEA alerting/warning application that is made available for download by the public on the common app stores. The public, through lack of understanding the WEA service, may be led to believe these apps are the ‘legitimate” WEA applications. The outside actor plays the role of an alert originator and sends whatever false alerts they wish to the public which confuses members of the public into believing that such alerts received through the bad app are real WEA alerts.

The IPAWS Open Platform for Emergency Networks (OPEN) validates the messages Alert Originators send, convert the message to a format used by CMSPs, and then send the message to connected CMSPs. Of primary concern for this CSRIC V effort is the method IPAWS uses to validate alert messages, the process for granting Alert Originators’ access, the IPAWS-OPEN software code base, and the logical connectivity with CMSPs. In addition to the DHS Sensitive Systems Policy Directive 4300A requirements, the FEMA IPAWS Program Management Office sought the assistance of the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to enhance the security posture of the IPAWS-OPEN system. The ICS-CERT conducted an on-site design architecture review and assessment of the IPAWS-OPEN system and recommended areas of focus which are consistent with the content of this report.

The CMSP networks are vulnerable to alert originators with malicious intent performing a DOS attack on all cellular operator networks in a given alert area (including nation-wide) by sending phone numbers and/or URLs in false WEA alerts that will either:

* Cause alert recipients to click on the URLs perhaps leading to extremely slow public or private servers, or worse, to virus-infected links that could lead to all sorts of issues with user devices (including ransomware, Trojans, or subject the recipient to premium text messaging services) and operator networks, or
* False alerts could recommend clicking on phone numbers that are advertised in the message to connect the user to “critical information for public safety” but may in fact connect to premium service numbers.

In either scenario, many users attempting to call the phone number or open the URL will result in cellular networks quickly congest, and the ability of users to make/receive phone calls will be significantly hampered if such alerts are sent to the public.

3GPP TS 22.268 (Public Warning System Requirements) generated by 3GPP SA1 (Requirements working group), and 3GPP TR 33.969 (Study on Security Aspects of PWS) generated by 3GPP SA3 (Security working group) included options for digital signatures/encryption methods for securing alerts from the risk of malicious actors deploying a false cellular base station that could perform broadcasts on operator spectrum of WEA alerts to users within its RF coverage.

As part of the WEA pipeline, CMSP networks contain the CMSP Gateway, as well as underlying cell broadcast elements. One very unlikely threat vector is where the attacker must be able to gain access to the appropriate computer or network server in order to modify or introduce malicious code, deliver a payload, or create a malicious outcome. CMSPs have very strict security procedures in place for modifying software on any mission critical element in the network. These procedures include testing and certification of the software/software updates, and planning for and implementing the installation of the software according to an established procedure. Access to the systems, including physical access, is tightly controlled.

PBS WARN is a safeguard to ensure delivery of the WEA, even in the event that a cybersecurity or other event disrupts the primary WEA delivery path.

Based on the WEA security analysis conducted in Working Group 2, it is our conclusion that additional security measures as described in the Recommendation section of this report may mitigate security threats identified in this report. To that end, it is recommended that the industry, FEMA, DHS, and Alert Originators collaborate on the development a new Best Practices standard in ATIS.

# Introduction

The Wireless Emergency Alerts (WEA) service is a collaborative partnership that includes the cellular industry, Federal Communications Commission, Federal Emergency Management Agency (FEMA), and U.S. Department of Homeland Security Science and Technology Directorate. The WEA capability provides a valuable service, disseminating imminent threat emergency alerts to users of capable mobile devices if they are located in or travel into an affected geographic area. However, like other cyber-enabled services, WEA may be subject to cyber threats that may prevent its use or damage the credibility of the service it provides.

This report reviews the current WEA security practices and recommends actions, which may include development of best practices, to CSRIC.

## CSRIC Structure

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Communications Security, Reliability, and Interoperability Council (CSRIC) V**  **CSRIC Steering Committee - Working Group Structure** | | | | | | | | |
| Susan Sherwood  Jeff Cohen  (Co-Chairs) | Francisco Sanchez  Farrokh Khatibi  (Co-Chairs) | Steven Johnson  Kelly Williams  (Co-Chairs) | Kent Bressie  Catherine Creese  (Co-Chairs) | Jennifer Manner  (Chair) | Rod Rasmussen  Chris Boyer  Brian Allen  (Co-Chairs) | Brian Scarpelli  Joel Molinoff  (Co-Chairs) | Bill Boni  Drew Morin  (Co-Chairs) | William Reidway Jr.  Thomas Anderson  (Co-Chairs) |
| **Working Group 1**: Evolving 911 Services | **Working Group 2**: Emergency Alerting Platforms | **Working Group 3**: Emergency Alert System | **Working Group 4**: Communications Infrastructure Resiliency  **Sub-Group A**: Submarine Cable Resiliency | **Working Group 4**: Communications Infrastructure Resiliency  **Sub-Group B**: Network Timing Single Source Risk Reduction | **Working Group 5**: Cybersecurity Information Sharing | **Working Group 6**: Secure Hardware and Software – Security-by-Design | **Working Group 7**: Cybersecurity Workforce | **Working Group 8**: Priority Services |

Table 1 - Working Group Structure

## Table - Working Group Structure

## Working Group 2 Team Members

Working Group 2 consists of the members listed below.

|  |  |
| --- | --- |
| **Name** | **Company** |
| Farrokh Khatibi, Co-Chair | Qualcomm Technology Inc. |
| Francisco Sánchez, Jr., Co-Chair | Harris County, Texas |
| Chris Anderson | FCC |
| Greg Cooke | FCC |
| James Wiley | FCC |
| Hutch McClendon | Advanced Computer and Communications |
| Brian Daly | AT&T |
| Peter Musgrove | AT&T (ATIS) |
| Caitlin Shockey | Centers for Disease Control |
| James Tyson | Centers for Disease Control |
| Jose Rivera | DHS |
| Denis A. Gusty | DHS, S&T/FRG |
| Alexander Gerdenitsch | Echostar |
| Jennifer Manner | Echostar |
| Scott Enright | Emmis Communications |
| Christopher Tarantino, MEP CMCP | Epicenter Media & Training |
| Alfred Kenyon | FEMA IPAWS |
| Mark Lucero, CISSP | FEMA IPAWS |
| Matthew Straeb | GSS Net |
| Brian Murray | Harris County Office of Homeland Security & Emergency Management |
| Tony Surma | Humanitarian Toolbox |
| Bob Sherry | Intrado |
| David Layer | NAB |
| Larry Walke | NAB |
| Mike Gerber | NOAA/NWS |
| Robert Bunge | NOAA/NWS |
| Steve Mace | NCTA |
| Dana Golub | PBS |
| Mark D. Annas | Riverside (CA) Fire Dept |
| Carol Woody | Software Engineering Institute |
| Brad Gaunt | Sprint |
| John Davis | Sprint |
| Keith Bhatia | TCS |
| Shelley Blakeney | T-Mobile |
| Tim Dunn | T-Mobile |
| Taelor Hardesty | University of Houston |
| Jeannett Sutton | University of Kentucky |
| Larry Rybar | Verizon |

Table 2 - List of Working Group Members

# Objective, Scope, and Methodology

## Objective

The objective of the Security SWG of CSRIC V WG2 is to review current Wireless Emergency Alert (WEA) security practices and recommend actions, which may include the development of best practices. The review will cover end-to-end security aspects of WEA including the integrity of all interfaces, insuring the integrity of the WEA message as it transverses from the alert originators and across the carrier networks, and security of message data on handsets. Consideration will be given to new technologies and cyber risks to WEA.

## Scope

The scope of this report is limited to the current standards-defined and deployed Wireless Emergency Alert (WEA) system. The security aspect of non-WEA systems, as well as enhancements to WEA under consideration[[1]](#footnote-1) are outside the scope of this report.

## References and Definitions

### References

1. FCC 08-99, *Federal Communications Commission First Report and Order In the Matter of The Commercial Mobile Alert System*; April 9, 2008.[[2]](#footnote-2)
2. *Federal Communications Commission (FCC) Commercial Mobile Alert System (CMAS) Notice of Proposed Rulemaking (NPRM)*, Docket 07-287; December 14, 2007.1
3. FCC 08-164, *Federal Communications Commission Second Report and Order and Further Notice of Proposed Rulemaking In the Matter of The Commercial Mobile Alert System*; July 8, 2008.1
4. FCC 08-184, *Federal Communications Commission Third Report and Order and Further Notice of Proposed Rulemaking In the Matter of The Commercial Mobile Alert System*; August 7, 2008.1
5. FCC 07-114, Federal Communications Commission Fourth Report and Order In the Matter of Wireless E911 Location Accuracy Requirements; February 3, 2015.1
6. *Common Alerting Protocol, v. 1.1; OASIS Standard CAP-V1.1*; October 2005.[[3]](#footnote-3)
7. J-STD-100, *Joint ATIS/TIA CMAS Mobile Device Behavior Specification*; January 30, 2009.[[4]](#footnote-4)
8. J-STD-100.a, *Supplement A to J-STD-100, Joint ATIS/TIA CMAS Mobile Device Behavior Specification*, December 2012.3
9. *Wireless Emergency Alerts Cybersecurity Risk Management Strategy for Alerts Originators*. Software Engineering Institute, Carnegie Mellon University.[[5]](#footnote-5)
10. Cybersecurity Framework Version 1.0, NIST[[6]](#footnote-6)
11. Ronald S. Ross, Guide for Conducting Risk Assessments, Special Publication (NIST SP) - 800-30 Rev 1.[[7]](#footnote-7)
12. Guide for Applying Risk Management Framework to Federal Information, Special Publication (NIST SP) -800-37 revision 1.[[8]](#footnote-8)
13. Ronald S. Ross, Managing Information Security Risk: Organization, Mission, and Information System View, Special Publication (NIST SP) - 800-39[[9]](#footnote-9)
14. Security and Privacy Controls for Federal Information Systems and Organizations, Special Publication (NIST SP) - SP 800-53 Rev. 4[[10]](#footnote-10)
15. DHS Sensitive Systems Policy Directive 4300A, Version 8.0[[11]](#footnote-11)
16. Federal Information Processing Standard Publication 199 (FIPS 199)[[12]](#footnote-12)
17. 3GPP TS 22.268, *Public Warning System (PWS) requirements.*[[13]](#footnote-13)
18. 3GPP TS 33.969, *Study on security aspects of Public Warning System (PWS).12*
19. J-STD-101, *Joint ATIS/TIA CMAS FEDERAL ALERT GATEWAY TO CMSP GATEWAY INTERFACE SPECIFICATION*. 4
20. J-STD-102, *Joint ATIS/TIA CMAS FEDERAL ALERT GATEWAY TO CMSP GATEWAY INTERFACE TEST SPECIFICATION*. 4

### Definitions

The following definitions are taken from the *FCC First Report and Order for the Commercial Mobile Alert System* [Ref 1]:

**Alert Message**: An Alert Message is a message that is intended to provide the recipient information regarding an emergency, and that meets the requirements for transmission by a Participating Commercial Mobile Service Provider as defined in the *FCC First Report and Order for the Commercial Mobile Alert System*.

**Common Alerting Protocol**: The Common Alerting Protocol (CAP) refers to *Organization for the Advancement of Structured Information Standards (OASIS) Standard CAP-V1.1*, October 2005 [Ref 6], or any subsequent version of CAP adopted by OASIS and implemented by the CMAS.

**Commercial Mobile Service Provider**: A Commercial Mobile Service Provider (CMSP or CMS Provider) is an FCC licensee providing commercial mobile service as defined in section 332 (d)(1) of the Communications Act of 1934 (47 U.S.C. 332(d)(1)). Section 332(d)(1) defines the term commercial mobile service as any mobile service (as defined in 47 U.S.C. 153) that is provided for profit and makes interconnected service available: (a) to the public; or (b) to such classes of eligible users as to be effectively available to a substantial portion of the public, as specified by regulation by the Federal Communications Commission.

# Background

The Wireless Emergency Alerts (WEA) service is a collaborative partnership that includes the cellular industry, Federal Communications Commission, Federal Emergency Management Agency (FEMA), and U.S. Department of Homeland Security Science and Technology Directorate. The WEA capability provides a valuable service, disseminating imminent threat emergency alerts to users of capable mobile devices if they are located in or travel to an affected geographic area. However, like other cyber-enabled services, WEA may be subject to cyber threats that may prevent its use or damage the credibility of the service it provides. Attackers may attempt to delay, destroy, or modify alerts, or even to insert false alerts, resulting in actions that may pose a significant risk to the public. Non-adversarial sources of failure also exist (e.g., design flaws, user errors, acts of nature that compromise operations).

## WEA Decomposition

As shown inFigure 1, the end-to-end WEA pipeline consists of the following four major elements that implement the alerting process:

* *Alert originators*: the people, information, technology, and facilities that initiate and create an alert, define a target distribution area (i.e., targeted geographic area), and convert the alert information into the appropriate format for dissemination
* *Integrated Public Alert and Warning System (IPAWS)*: a collection of FEMA systems that receive, validate, authenticate, and route various types of alerts to the appropriate disseminator, such as WEA, the Emergency Alert System, or the National Oceanic and Atmospheric Administration
* *Commercial mobile service providers (CMSPs)*: participating commercial wireless carriers that broadcast WEA messages to a designated geographic area
* *Alert recipients*: the WEA-capable mobile devices located in the targeted alert area

Figure - The Four Elements of the WEA Pipeline

Alert Originators

IPAWS

CMSPs

Alert Recipients

## Potential Security Risks

This section discusses potential security risk scenarios and the use of an analysis technique developed by researchers at the Software Engineering Institute [Ref 9]for evaluating and addressing these risks. Once each scenario is described, the next step is to analyze the risk to determine its probability of occurrence and impact on each of the elements of the WEA service. This information will be used to prioritize the risks and identify appropriate mitigations. This prioritized ranking of the risk scenarios provides a basis for recommending administrative, technical, and/or physical security controls.

The following risk scenarios were identified in a study of CMSPs conducted by the Software Engineering Institute and funded by DHS [Ref 9] as well as other sources:

* Risk 1: Insider Sends False Alerts
* Risk 2: Inherited Replay Attack
* Risk 3: Malicious Code in the Supply Chain
* Risk 4: Denial of Service
* Risk 5: Outsider Sends False WEA Alerts
* Risk 6: Insider Blocks Real WEA Alerts
* Risk 7: Outsider Blocks Real WEA Alerts
* Risk 8: CMSP Infrastructure Testing System Access
* Risk 9: Security Vulnerability in Existing Standards

These scenarios provide a broad cross section of the types of issues likely to affect the elements of the WEA chain; furthermore, there could be additional scenarios that may be more specific to the other elements of the WEA chain.

The underlying threats that trigger these risk scenarios include an insider (Risk 1), the consequences of an upstream attack on an Alert Originator (Risk 2), malicious code inserted in the CMSP supply chain (Risk 3), and a denial-of-service attack (Risk 4). While not exhaustive, the resulting analysis provides a broad range of mitigation techniques that should be considered. The remainder of this section describes each risk scenario in detail and highlights the ranking of those scenarios based on risk exposure.

### Risk 1: Insider Sends False Alerts

An insider is employed by one of the stakeholders (e.g., Alert Originator, FEMA, CMSP, etc.). The insider could be a software developer who is responsible for developing applications or related software to implement WEA in one of the pipeline elements.

One potential attack vector is for a disgruntle insider to plant a logic bomb in the WEA system, hoping to send “custom” WEA messages to all WEA-capable wireless devices within the targeted geographic area. There are three potential threat vectors in the WEA pipeline:

1. At one of the many Alert Originator sources, or
2. At the FEMA IPAWS system, or
3. At a CMSP gateway of one of the participating CMSPs

The “disgruntled insider’s” ultimate goal could be to create mass public confusion, divert attention from some other unrelated planned attack at the same time or to bring negative publicity to the emergency management agency, the commercial mobile service provider, FEMA, and/or to WEA in general. As a function of his job, the insider must have unlimited access to the appropriate system in the WEA pipeline, and must be able to gain access to the appropriate computer or network server in order to modify or introduce malicious code, deliver a payload, or create a malicious outcome. As an example, while on site and during work hours, the insider develops a logic bomb designed to replay a nonsense WEA message repeatedly.

Once the logic bomb is triggered, the malicious WEA message goes out to many recipients. If the attack occurs in the Alert Originator or IPAWS elements of the pipeline, it is likely that recipients of the malicious message would be for all participating CMSPs and limited to the geographic area within the alert originator’s jurisdiction or significantly larger if the attack occurs within the FEMA IPAWS; if the attack occurs at the CMSP, then the recipients of the malicious message may be limited to those of the attacked CMSP, but the geographic area may be significantly larger (potentially the entire CMSP coverage area).

The result of this attack is many recipients become annoyed at receiving the same alert repeatedly. Some of these people complain to the carrier’s customer service representatives, or may call 9-1-1 or their local emergency management for further information on the message or to complain about the receipt of the malicious messages. A large number of recipients may turn off the WEA function on their phones in response to the attack.

If a single participating CMSP is attacked, there is a potential impact that some customers leave their operator for other operators, although this churn may statistically occur evenly across all operators, assuming the attack was sent to all CMSPs in the geo-targeted area.

In addition, many people lose trust in the WEA service. Many of these recipients will permanently disable the WEA service on their mobile devices after experiencing this attack.

All WEA messages, even if spoofed, will have an origination point. The current feedback mechanisms to alert originators are limited and require them to actively monitor a data feed to determine if a message originated by their systems has been received by FEMA IPAWS. It could be useful to expand the information on this data feed to include whether FEMA IPAWS has distributed the WEA message to the Participating CMSPs. Alert originators identifying a message when they did not send an alert would be able to send a correction (such as an alert cancellation if it was originated from their systems) or quickly recognize a problem. Additional monitoring capabilities that use the alert notification confirmation data could also identify mismatches between sent and distributed messages and increase the likelihood of earlier problem identification for this type of risk.

### Risk 2: Inherited Replay Attack

An attacker targets an Alert Originator (AO) to capture legitimate WEA messages (unencrypted) and their associated AO certificates (encrypted) during transmission. She intends to resend a legitimate alert repeatedly at a later time (i.e., a replay attack), hoping to annoy people who use the WEA service. The attacker captures multiple WEA messages and selects one that will affect a large number of people, based on the geographic area targeted by the alert message.

At a later time, the attacker executes a replay attack using the captured WEA message (i.e., now considered to be an illegitimate alert). She sends the illegitimate alert (unencrypted) and associated AO certificate (encrypted) to IPAWS-OPEN, which then performs the following activities:

* accepts the illegitimate alert
* confirms the source as legitimate using the AO certificate
* processes the illegitimate alert
* forwards the illegitimate alert to the CMSP Gateway for all participating CMSPs, along with the appropriate certificate

The attacker then repeatedly sends the same illegitimate alert to IPAWS-OPEN, which processes each alert and forwards it to all participating CMSP Gateways. Each illegitimate alert is accepted by the CMSP Gateways and validated as being legitimate.

As a result of this attack, many customers will contact customer care of their CMSP, and/or contact 9-1-1 or their local emergency management agency to report the messages. Others may leave their operator for other operators, although this churn may statistically occur evenly across all operators, as the attack was sent to all participating CMSPs in the geo-targeted area. In addition, many people lose trust in the WEA service. Many of these recipients will permanently disable the WEA service on their mobile devices after experiencing this attack.

### Risk 3: Malicious Code in the Supply Chain

An employee at a subcontractor of one of the stakeholders (e.g., Alert Originator, IPAWS, CMSP, etc.) decides to execute an attack, for reasons not relevant to this study. The subcontractor’s technical staff completes development and testing of the software update for a computing or network server component in the WEA pipeline. The employee who wants to execute the attack modifies or introduces malicious code to create a malicious outcome with the inserted code, and delivers it to the customer (Alert Originator, IPAWS or CMSP). Technical staff from the customer’s development team do not detect the malicious code during testing and acceptance the software update.

The malicious code may expand the region receiving the alert as broadly as possible, change the alert content, or even change the priority of the alert , for example into a Presidential alert.

As a result of the attack, many customers will contact customer care of their CMSP, and/or contact 9-1-1 or their local emergency management agency to report the messages. Others may leave their operator for other operators, although this churn may statistically occur evenly across all operators, assuming the attack was sent to all participating CMSPs in the geo-targeted area.

Because of the high-profile nature of the attack (i.e., issuing illegitimate Presidential alerts), the media covers the attack extensively. The media coverage of the attack helps to amplify the public’s loss of trust in the WEA service.

### Risk 4: Denial of Service

An outside actor with malicious intent is planning a physical (i.e., terrorist) attack on a crowd that is gathered in a public place (e.g., for a sporting event or concert). She plans to conduct a simultaneous denial-of-service (DoS) attack on all participating CMSPs WEA alerting system to prevent the dissemination of a WEA message about the attack. The goal is to prevent people from learning about the physical attack as long as possible in order to maximize the physical harm inflicted up-on the crowd.

The actor targets a third-party contractor that has legitimate access to the stakeholders (e.g., alert originator, IPAWS, CMSP, etc.) internal network. She performs additional reconnaissance on the infrastructure to get information needed to gain access. The third-party contractor is not vigilant about its cybersecurity practices and is a relatively easy target for an attacker.

The actor instructs the infected computers at the contractor to send a flood of WEA alerts, which may consume the system’s available bandwidth at some elements of the WEA chain. When an Alert Originator enters a legitimate WEA message, it may not reach the Alert Recipients because the system’s bandwidth is consumed by the DoS attack at one of the WEA chain elements.

The cost to recover from the attack is considerable. Media outlets learn about the DoS attack’s role in amplifying the impact of the incident and publicize this fact in their reports. The reputation of the operator could be damaged with the general public, leading to a loss of business, although this churn may statistically occur evenly across all operators, assuming the attack was sent to all CMSPs in the geo-targeted area. Finally, many people lose trust in the WEA service.

### Risk 5: Outsider Sends False WEA Alerts

An outside actor with malicious intent gains access to one of the systems in the WEA pipeline used to create/disseminate WEA alerts (e.g., Alert Originator or IPAWS). This could include connecting to an alert origination system, the IPAWS system, a CMSP system, or the device itself (e.g., through malicious SMS messages or through third party applications that mimic WEA alerts). Generally, the same downsides as described for the other risks above apply in this scenario.

### Risk 6: Insider Blocks Real WEA Alerts

An insider with malicious intent gains access to any of the systems related to WEA (from alert origination systems, IPAWS, CMSPs) and purposefully prevents a valid WEA alert from being sent to the next “stage”, or in the case of the device, causes the alert not to be presented/displayed as a proper WEA alert.

### Risk 7: Outsider Blocks Real WEA Alerts

An outsider with malicious intent poses as one of the systems in the route of a normal WEA alert. Their intent is to block valid WEA messages from moving down the pipeline and therefore the result is a blocking of a valid WEA alert to the public.

### Risk 8: CMSP Infrastructure Testing System Access

An imposter having access to the CMSPs WEA test system could potentially open an attack vector similar to having access to the production environment. Most carriers have the ability to send test alerts from their environment, however the test environment is not connected to RAN elements in production and no broadcast can leak into production. In addition, users of the system have different levels of access. The testers that have access to the test tool cannot generate “live” alert messages using the WEA message identifiers, and have read only access to the network element database as well since that information is generally needed to construct the test alert, but this is not sensitive information. There is generally no way for someone with access to the test system to send an alert with anything other than a test message ID. Real Alerts must be received from the IPAWS Alert Gateway

The testers are also unable to change the test message text, and test messages are set to broadcast, for example, “This is a TEST of the Commercial Mobile Alert System. This is only a Test.” Only a full administrator can change the text of that message for the test IDs.

That said, a tester could potentially initiate a denial of service attack by generating a significant number of test alerts. So, unauthorized access to the test tool, may pose a low risk threat to the security of the CMSP network.

### Risk 9: Security Vulnerability in Existing Standards

The WEA networks and end-user devices face an array of threats that may seek to take advantage of potential vulnerabilities. It is important to adopt adequate security patching policies across all the elements of the WEA pipeline. As an example, the C-interface requires a VPN IPsec tunnel. Any security hole that exists will depend on the security quality of the VPN tunneling algorithm itself, i.e. a hijacker gaining access to the VPN tunnel will result in the entire WEA system being compromised. Therefore, the owners of the elements in the WEA pipeline must be encourage to continue to be vigilant in mitigating protocol security vulnerabilities to ensure that all WEA related systems and software are up to date.

## Risk-Based Analysis

A risk-based analysis is a useful approach for prioritizing which controls to address first. National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, titled *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, defines more than 200 hundred controls across 18 categories [Ref 14]. In order to limit the number of controls to a manageable subset, NIST recommends a risk-based approach for identifying high-priority controls [Ref 9] [Ref 10] [Ref 11] [Ref 12] [Ref 13]. In this way, the focus can be initially on the subset of controls that mitigate the highest priority cybersecurity risks. This study applied a prioritization approach.

In the previous section, several potential risks were identified. The next step is to analyze these potential risks based on key criteria:

* Probability
* Impact
* Risk exposure

Once the analysis is completed and controls are selected, recommendations will be proposed to mitigate each risk. It is important to note, because the impact of each risk will vary across the pipeline, that each element of the WEA chain will need a separate risk-based analysis and recommendations for a mitigation plan.

## Security Analysis of the Elements in WEA Chain

In this section, each element of the WEA chain will be analyzed.

### Alert Originators

Alert Originators are those authorized federal, state, territory, tribal, and local organizations that initiate WEA messages. Alert Originators utilize software to craft their alerts, digitally sign their alerts (see section 4.4.2.1), and send them to the next element in the WEA pipeline, IPAWS. There are a number of important security measures required to prevent unauthorized WEA activations. These can be summarized in three key categories: People, process, and software. It is through the application of sound security practices in each of these categories that the Alert Originators can safeguard their interest in WEA.

#### People

The person who creates an alert is most likely not the IT security professional for the organization. They may not be the one who signs the legal agreement with FEMA for use of the system. Therefore, an emergency management agency with WEA origination capability must understand the implications of the legal agreement they signed for access, how it extends to the staff, and the effects of a security compromise. The effects are not only to the agency, but to the entire WEA system. The public trust and confidence in the system erodes if the alerts that people receive are not legitimate. The primary security concerns of the people involved in Alert Origination are in safeguarding passwords and digital certificates.

The FEMA Memorandum of Agreement and Rules of Behavior require the use of strong passwords and forbid password sharing. This applies to the Alert Originator’s access to their alerting software. Most alerting software in use today is web-based, meaning that anyone with an Internet connection can get to the login screen. A strong password could be all that prevents a bad actor from sending an unauthorized WEA to the entire county, state, or applicable area of responsibility.

The digital certificate is quite literally the key required to send an alert. FEMA maintains the chain of custody for handling certificates down to the person(s) authorized in the MOA. From that point it is the Alert Originator’s responsibility to safeguard the digital certificate once they take possession. The Alert Originator should only contract with an alerting software vendor that they trust, because the digital certificate is usually uploaded into the vendor alerting software tools.

#### Process

The Alert Originator is responsible for making policy for how their agency will use WEA. In some instances, the state will provide assistance through existing plans, policies, or statutes. The policy should detail how and when WEA is used and by whom. The absence of a documented policy creates a condition where access to the alerting software is not controlled or enforced. It also creates a void where guidance on proper use of the system should be documented. The agency needs to establish clear guidance for when WEA can be used (i.e., imminent threat and Amber Alerts vs. a WEA alert sent telling people not to park on Main Street because there will be a parade.). Finally, the documented policy and process must be instilled through training. The agency staff must exercise the policy in a training mode to address questions and concerns that may come up and prepare for timely use in an emergency.

In an effort to promote the development and use of alerting plans, FEMA makes template plans available to alerting authorities to tailor to their needs and adopt for their organization. A major focus of the templates is in coordination with neighboring jurisdictions before, during, and after the alerts are sent, as well as identifying the criterion used to determine when an alert will be sent. The templates were created by the Colorado Division of Homeland Security and Emergency Management, the Kentucky Division of Emergency Management, and the FEMA Chemical Stockpile and Emergency Preparedness Program. Plan templates and examples are available through the FEMA IPAWS Program Office.

#### Software

Many of the security responsibilities of the Alert Originator are addressed and applied through their alerting software tools. A vendor that employs a robust security program in their operation will help the Alert Originator to safeguard their access and prevent unauthorized WEA activations. A vendor that has a weak security program is putting the Alert Originator and the public they serve at risk. Some of the primary security concerns with alerting software tools are passwords, safeguarding the digital certificate, and defense in depth applied to their operation.

As most alerting software tools are web-based, it is imperative that they enforce strong passwords for access. Additionally, the software tool should employ a bad password count lock-out to discourage brute force attacks trying to systematically guess the password.

Safeguarding the digital certificate is critical. The most popular alerting software vendors may have up to 100 state and local alert originators as clients, all of whom upload their digital certificates to the vendor servers. Since the digital certificate is such a sensitive item, it is important that the alerting software vendor protect these assets at rest. A breech of their security containers could potentially allow a nefarious actor to send alerts to large geographic areas and to a large percentage of the US population. The way that digital certificates are invoked to sign alert messages must be secure as well. A poorly written routine that calls the digital certificate may make it vulnerable to compromise via extraction.

Finally, the alerting software vendors must exercise a defense in depth strategy to secure their assets. Application of firewalls, physical security, access control, patched and updated software, security policies, policy enforcement, and periodic review are essential to reducing the risk of exposing attack surfaces to would-be hackers. Additional security measures such as auditing, logging of user actions, non-repudiation, etc. should be considered.

A federally sponsored certification program could be used to validate the security procedures used by alerting software developers. A standard set of security requirements would need to be developed and socialized with the developer community. The developer would then submit their product to an independent, accredited test lab that would conduct code reviews, security scans, and either identify security gaps or certify the software for inclusion in a Certified Products List. In addition to security validation, the products could also be certified for conformance to the alerting standards and other alerting requirement that promote successful alert and warning messaging.

#### Malicious Warning App

This section is an expansion of Risk 5 in Section 4.2.5. An outside actor with malicious intent creates a non-WEA alerting/warning application that is made available for download by the public on the common app stores, or may be available via an Internet web site. The public, through lack of understanding the WEA service, may be led to believe these apps are the ‘legitimate” WEA applications. The app is developed such that alert messages received via the app have the same (or nearly the same) alerting tone or vibration cadence as legitimate WEA alerts. These alerts also are displayed on the device to look identical to a real WEA alert. The outside actor plays the role of an alert originator and sends whatever false alerts they wish to the public which confuses members of the public into believing that such alerts received through the bad app are real WEA alerts. Such alerts are not geo-targeted and are dependent on the public downloading the app to their device.

### IPAWS

The IPAWS Open Platform for Emergency Networks (OPEN) is an information system that acts as the gateway between Alert Originators and the CMSPs. The purpose of IPAWS-OPEN is to validate the messages Alert Originators send, convert the message to a format used by CMSPs, and then send the message to connected CMSPs. Of primary concern for this CSRIC V effort is the method IPAWS uses to validate alert messages, the process for granting Alert Originators’ access, the IPAWS-OPEN software code base, and the logical connectivity with CMSPs. In addition to the DHS Sensitive Systems Policy Directive 4300A requirements [Ref 15], the FEMA IPAWS Program Management Office sought the assistance of the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) to enhance the security posture of the IPAWS-OPEN system. The ICS-CERT conducted an on-site design architecture review and assessment of the IPAWS-OPEN system and recommended areas of focus which are consistent with the content of this report.

#### IPAWS Message Validation

Any government information system requires a measure of confidentiality, integrity, and availability suitable to the mission and in accordance with its Federal Information Processing Standard Publication 199 (FIPS 199 [Ref 16]) classification Public alert and warning messages are non-sensitive, public information, and consequently, there is no requirement for message confidentiality. There is, however, a need for assured message integrity (aka non-repudiation) and system availability. This is to ensure the alert message is not changed, and to ensure the system is online when needed.

Assured message integrity means there is a mechanism in place to prove that the message received was indeed created by the authorized Alert Originator and was not manipulated in transit or at rest. This integrity is accomplished through digitally signing the alert message at the origination point. An Alert Originator uses software to create an alert message in CAP XML [Ref 6] format, create a one-way hash of the XML, and then encrypt the hash using the Alert Originator’s private key. Anyone who receives the alert message XML can use the Alert Originator’s public key to decrypt the hash and compare it to that of the received message. If they are equal, then the message is authentic, if they are not equal, then the message was changed and should be rejected. IPAWS uses this method to ensure authenticity of the message received from the Alert Originator. IPAWS converts the message to a CMAC XML format message, FEMA digitally signs the message and sends it to the CMSP. The CMSP then uses FEMA’s public key to validate the authenticity.

CMAC

CAP

CMSP

IPAWS

Alert Originators

Figure – Message Validation

System availability is important for a public safety system as it must be online and working when needed. The IPAWS-OPEN system achieves high availability through two primary mechanisms. First, the IPAWS-OPEN system is fully redundant utilizing load balanced hardware, backup power, and redundant network components. Second, the IPAWS-OPEN system resides in multiple data centers with geographic diversity in an active-active configuration. If one data center goes down, the load is shifted to maintain operation.

#### IPAWS Alert Originator Access Process

Access to IPAWS-OPEN, and therefore the ability to originate WEA messages, is made available to federal, state, territory, tribal, and local government organizations. The vast majority of alert originators are local government entities. FEMA does basic vetting of the organization to begin the process, and the final authorizations are made by the state. In most cases this is the state emergency management agency, but could also include the state police or state homeland security division. Before access is granted, the state confirms the legitimacy of the local organization and validates that their alert and warning request is consistent with any existing state alert and warning plans, statues, or regulations.

In addition to the vetting process, the Alert Originator executes a Memorandum of Agreement (MOA) with FEMA and signs a Rules of Behavior (ROB) (see Appendix C for a sample). The MOA outlines the appropriate use, security concerns, and terms of the Alert Originator’s access to IPAWS-OPEN. The MOA is good for 3 years at which time both parties must agree to continue the relationship, else the agreement and access is terminated. The ROB outlines the specific requirements for strong passwords, data protection, and incident reporting. A potential risk is that the Alert Originator may not adhere to the terms of the MOA and ROB. To the maximum extent FEMA and Alert Originators rely on the sound security practices of the alerting software provider. Section 4.4.1 describes the related security analysis for the Alert Originator and alerting software provider relationship.

While the certificate-based message integrity described in section 4.4.2.1 works very well under ideal conditions, the potential for a certificate compromise does exist. The legal agreement between FEMA and the Alert Originator requires the Alert Originator to notify FEMA of any such security compromise. FEMA can then revoke the certificate and prevent misuse. The timeframe between the compromise and the corrective action creates a window of opportunity for unauthorized alert messages to be sent. Such a situation would require that a nefarious actor obtained the certificate during this window of opportunity.

The primary attack vectors for compromising the digital certificate include attacking the alerting software data at rest (described in section 4.4.1.3), and attacking the process for transmitting the digital certificate to the alerting authority. FEMA encrypts the digital certificate and then transmits it to the alerting authority via email. FEMA then provides the encryption password via voice call using the contact information provided by the alerting authority. An outside actor could intercept the email or hack the alerting authority’s email to obtain the encrypted certificate. They could then brute force attack the encryption to obtain the digital certificate. Alternative methods for transmitting the digital certificate include using a trusted third party escrow service, utilizing smart card tokens, classified email, and in-person verification.

#### IPAWS Software Code Base

Operating system and commercial software updates and patching are routine. While these update and patching activities prevent the exploitation of vulnerabilities, there are attack vectors which are not addressed through routine updates and patching. Malicious code can find its way into an information system through the hardware platform itself. The federal government has included awareness of these threats and mitigating measures to detect them as part of the required security certification and accreditation process. The hardware employed by FEMA information systems comes from controlled sources for which the supply chain is approved. For instance, it is not permitted to purchase a server from eBay and use it in the enterprise, regardless of updates and patches that may have been applied. Likewise, the IPAWS software code base is scanned using automated source code inspection toolsets. These tools ensure there is no latent malicious code in the custom IPAWS-OPEN code.

IPAWS-OPEN leverages the FEMA enterprise information technology components. These include both physical hardware and the enterprise software services architecture such as directory services, database services, and web services. While this creates efficiencies, there is some risk in relying on the enterprise. For instance, if several FEMA programs require a change to the enterprise in order to support their systems, IPAWS-OPEN will need to change as well. Similarly, if IPAWS-OPEN needs the enterprise to change, it will impact a change to other programs. All major changes are coordinated through the FEMA enterprise architecture review board, but changes may be slow. If it there is a change that impacts performance, the approval process could negatively impact the functionality of IPAWS-OPEN.

#### IPAWS Logical Connectivity

IPAWS-OPEN relies heavily on the Internet for connectivity among the multitude of state and local Alert Originators. It also relies on the Internet for connections to the CMSP gateways. Even though IPAWS-OPEN uses redundant and diverse connections, the Internet is still the common factor. A successful attack on the DNS root nameservers would slow or cease traffic between Alert Originators and IPAWS-OPEN, and traffic between IPAWS-OPEN and the CMSP gateways.

DHS uses the Trusted Internet Connection (TIC) concept for all external (i.e. non-DHS network) connectivity. IPAWS-OPEN takes advantage of the DHS TIC diversity and redundancy for communications with Alert Originators and with CMSP gateways. There is some risk in that these connections are not controlled by FEMA or the IPAWS program management office. While it has never happened, it is possible that the TICs may be shut down to protect the DHS network from an external cyber threat. This would isolate IPAWS-OPEN and render WEA unavailable. A more realistic threat would be an uncoordinated change to the TIC that negatively affect IPAWS-OPEN connectivity with external partners.

#### Blocking of Valid WEA Messages

This section expands on risk 7 in Section 4.2.7. An outsider with malicious intent poses as one of the systems in the route of a normal WEA alert. Their intent is to block valid WEA messages from moving down the pipeline and therefore the result is the blocking of a valid WEA alert to the public. In this case, the actor poses as an IPAWS system in the setup of a TCP connection with an alert origination system. The alert origination system believes it is sending an alert to IPAWS over the TCP connection to the outside actor which blocks real alerts from going to the real IPAWS system.

### CMSPs

#### Blocking of Valid WEA Messages

This section expands on risk 7 in Section 4.2.7. An outsider with malicious intent poses as one of the systems in the route of a normal WEA alert. Their intent is to block valid WEA messages from moving down the pipeline and therefore the result is the blocking of a valid WEA alert to the public. In this case, the actor poses as a CMSP gateway in the setup of a TCP connection with IPAWS. The IPAWS system believes it is sending an alert to a valid CMSP gateway over the TCP connection to the outside actor. In this case, the outside actor can mimic multiple CMSP gateways depending on how many TCP connections they can establish with IPAWS. This may be difficult for a malicious actor to perform as connection to IPAWS is a not a totally automated process. When a CMSP gateway connects to IPAWS, human beings and phone calls are part of the process.

#### Risks of false base station transmitting a false WEA alert

The existing 3GPP standards provide solutions to mitigate this risk. 3GPP TS 22.268 (Public Warning System Requirements) [Ref 17] generated by 3GPP SA1 (Requirements working group), and 3GPP TR 33.969 (Study on Security Aspects of PWS) [Ref 18] generated by 3GPP SA3 (Security working group) included options for digital signatures/encryption methods for securing alerts from the risk of malicious actors deploying a false cellular base station that could perform broadcasts on operator spectrum of WEA alerts to users within its RF coverage.

Section 4.8 of TS 22.268 contains the following requirements for the 3GPP Public Warning System (PWS), the international equivalent of WEA:

- PWS shall only broadcast Warning Notifications that come from an authenticated authorized source.

The following requirements only apply when not roaming internationally:

- When required by regional or national regulations, the integrity of the Warning Notification shall be protected. If no such regulatory requirement exists, there shall be no integrity protection of Warning Notifications, and all Warning Notifications shall be presented to the PWS application on the PWS-UE.

- When required by regional or national regulations, the PWS shall protect against false Warning Notification messages. If no such regulatory requirement exists, there shall be no protection against false Warning Notifications, and all Warning Notifications shall be presented to the PWS application on the PWS-UE.

Note 1: These requirements are subject to regulatory policies.

NOTE 2: The authentication and authorisation of the source are outside the scope of 3GPP Specifications.

#### Inclusion of URLs and phone numbers used for DOS attacks

The CMSP networks are vulnerable to alert originators with malicious intent performing a DOS attack on all cellular operator networks in a given alert area (including nation-wide) by sending phone numbers and/or URLs in WEA alerts that will either:

* Cause alert recipients to click on the URLs perhaps leading to extremely slow public or private servers, or worse, to virus-infected links that could lead to all sorts of issues with user devices (including ransomware, Trojans, or subject the recipient to premium text messaging services) and operator networks.
* Could recommend clicking on phone numbers that are advertised in the message to connect the user to “critical information for public safety” but may in fact connect to premium service numbers.

In either scenario, many users attempting to call the phone number or open the URL will result in the cellular data networks quickly congesting, and the ability of users to make/receive phone calls will be significantly hampered if such alerts are sent to the public. This represents a significant security threat and thus it is recommended that CMSPs reject any WEA message which contains a phone number or URL.

#### Risk of injecting false WEA alerts into operator equipment

Cellular operators may be vulnerable to insiders or outsiders with malicious intent gaining access to operator equipment and injecting false WEA alerts. However, existing operator security practices and access control mechanism minimize these risks. Injection of false WEA alerts into a CMSP gateway, a Cell Broadcast Center (CBC) are theoretically possible but very unlikely. Operators typically deploy WEA elements (CMSP Gateway, CBC) in secure data centers which have tight physical access controls (building security, credentialed access, monitoring, etc.). In addition, the computer and network server equipment running the WEA software is access controlled (required authorization to access the systems, password protection, etc.) to those that have a legitimate need for access to the equipment. Injection of false WEA alerts into Radio Access Network (RAN) nodes is not viewed as feasible for either insiders or outsiders.

In addition, CMSPs may generate logs of WEA alerts received from the IPAWS gateway which may be reviewed to identify malicious attacks.

#### Risk of injecting malicious software into a CMSP WEA component

As part of the WEA pipeline, CMSP networks contain the CMSP Gateway, as well as underlying cell broadcast elements. Risk 1 (section 4.2.1, Insider Sends False Alerts) describes a threat vector where the attacker must be able to gain access to the appropriate computer or network server in order to modify or introduce malicious code, deliver a payload, or create a malicious outcome. CMSPs have very strict security procedures in place for modifying software on any mission critical element in the network. These procedures include testing and certification of the software/software updates, and planning for and implementing the installation of the software according to an established procedure. Access to the systems, including physical access, is tightly controlled as described in 4.4.3.4. Thus, the threat vector described is very unlikely.

### Alert Recipients

#### Malicious Warning App

This section is an expansion of risk 5 in Section 4.2.5. An outside actor with malicious intent creates an alerting/warning application that is made available for download by the public on the common app stores, or available on an Internet web site. The app is developed such that alert messages received via the app have the same (or nearly the same) alerting tone or vibration cadence as real WEA alerts. These alerts also are displayed on the device to look identical to a real WEA alert. The outside actor plays the role of an alert originator and sends whatever false alerts they wish to the public which confuses members of the public into believing that such alerts received through the bad app are real WEA alerts. Note that this case spans both the alert originator and alert recipient categories. This risk is very difficult to detect and deter. The public can download anything they want and it does not even have to come from an “official” app store.

### PBS WARN

#### Background

PBS WARN provides a diverse and reliable backup to the primary Wireless Emergency Alert (WEA) system, with a fully redundant system design that leverages Public Television’s (PTV) nationwide coverage to send every WEA message over every PTV transmitter, covering virtually all of the United States and its territories.

CMSPs receive the primary distribution of WEAs over a secure Internet connection between the CMSP’s data center and FEMA. Public television (PTV) stations provide a redundant path for WEAs, leveraging broadcast’s one-to-many satellite distribution and terrestrial broadcasting to reach the same CMSP’s data centers over-the-air. PBS WARN ensures that the WEA reaches the CMSP, even in the event that the connection between FEMA and the CMSP is disrupted.

#### The importance of PBS WARN to WEA Cybersecurity

“Recognizing that the national and economic security of the United States depends on the reliable functioning of critical infrastructure, the President issued Executive Order (EO) 13636, [Improving Critical Infrastructure Cybersecurity](http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity), in February 2013. The Order directed NIST to work with stakeholders to develop a voluntary framework – based on existing standards, guidelines, and practices - for reducing cyber risks to critical infrastructure. The Cybersecurity Enhancement Act of 2014 reinforced NIST's EO 13636 role.”[[14]](#footnote-14)

The Framework for Improving Critical Infrastructure Cybersecurity (“Framework”) [Ref 10] sets forth five core functions, which are “not intended to form a serial path, or lead to a static desired end state. Rather, the Functions can be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk.” One such core function is to Protect, defined by the Framework as intended to “develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.”

PBS WARN is a safeguard to ensure delivery of the WEA, even in the event that a cybersecurity or other event disrupts the primary WEA delivery path.

The PBS WARN system is not only optimized for maximum availability, but is also technologically diverse from WEA’s primary path. Technological diversity mitigates the risk resulting from complete dependence upon a single technology stack that contains unidentified design defects, security vulnerabilities, or operational weaknesses.

In the event of a cybersecurity incident at a carrier facility, the PBS WARN system is well positioned to provide an immediate alternate source of inbound WEA messages.[[15]](#footnote-15)

#### Diversity

The PBS WARN system achieves diversity in three different domains: (1) physical layer diversity (2) logical layer diversity, and (3) time diversity.

The physical layer of the PBS WARN system is a radio-frequency (RF) over-the-air interface operating in a one-to-many broadcast mode. In contrast to the primary WEA interface, the physical layer does not rely on inbound copper or fiber circuits at the CMSP facility. This technological difference protects against physical attacks and power failures external to the CMSP facility.

The logical layer of the PBS WARN system is a packetized data stream formatted according to MPEG digital video industry standards (with some additional metadata specific to the PBS WARN system). In contrast to the primary WEA interface, the logical layer does not rely on source or destination MAC or IP addresses to assure routing and delivery. This technological difference protects against failures or attacks on core Internet protocols such as BGP or DNS.

The time domain of the PBS WARN system incorporates a periodic, repeating “carousel” of messages to further ensure message delivery in cases where time diversity may be required to overcome a brief system interruption from an external natural or man-made event.

#### Availability

Individual components and sub-systems that operate within the PBS WARN system are optimized for availability in accordance with industry best practices. The system design includes hot spares with automatic failover, an automated health monitoring system, and a completely separate backup facility in a geographically diverse location. These measures may be considered industry best practice for any system that requires high availability. However, beyond these industry-standard best practices for system operation, the PBS WARN system includes several inherent design characteristics that further enhance availability at the CMSP facility:

1. The inherent one-to-many broadcast architecture results in a system, which can accommodate any number of CMSP subscribers with no negative performance or availability impact. Availability is independent of subscriber load.
2. Conventional Denial of Service (DoS) attacks are largely mitigated by a session-less one-way communications channel. Ping-of-death, SYN flood, and similar attacks rely on a session oriented two-way communications channel. The PBS WARN interface to CMSP’s cannot be attacked using these methods since there is no return communications channel.
3. Remotely launched DoS attacks are also mitigated since there is no reliance on a public IP address at CMSP facility edge. Attackers cannot launch a DoS attack against the CMSP’s interface to the PBS WARN system without access to the physical layer, which would require an attacking device with physical proximity to the CMSP facility.

#### How Does a CMSP Utilize WARN as a Backup?

Any CMSP that has been authorized by FEMA to distribute WEA messages may use PBS WARN as a no-cost backup with no additional approval or paperwork required, as shown in Figure 3.

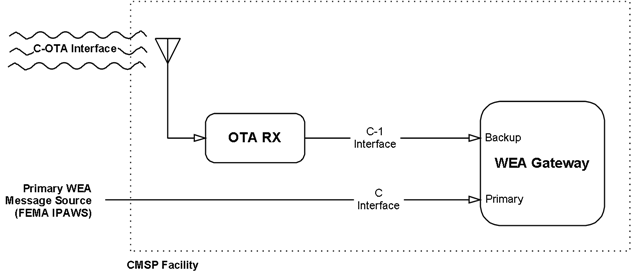
****

Figure - PBS WARN Redundancy

To utilize PBS WARN as redundant source of WEA messages, CMSPs must establish connectivity with the C-1 interface, which was developed by ATIS/TIA specifically for use with the PBS WARN system and is defined within ATIS J-STD-101 [Ref 19].

The C-1 interface is intended for implementation with conventional technology stacks such as Ethernet and TCP/IP. As such, C-1 does not interface directly with the RF signal broadcast over-the-air by PBS broadcast stations. An over-the-air receiver (“OTA RX”), is necessary to perform the signal processing required to convert the inbound RF physical layer/MPEG logical layer from PBS broadcast stations into the form specified by J-STD-101 C-1. The OTA RX performs physical layer translation, logical layer translation, and also performs other important processing functions such as duplicate message identification. The OTA RX connects to a CMSP’s WEA Gateway’s alternate message input port using the C1 interconnect standard.

PBS maintains a free, publicly available document, which describes the recommended functionality and processing functions of the OTA RX. [[16]](#footnote-16)

# Findings and Recommendations

## Findings

Following are some findings based on the work done in CSRIC V WG2:

1. The current system is handling expected WEA alerting as designed.
2. There is an understanding that each participant in the WEA pipeline bears some responsibility for making the entire pipeline effective and secure.
3. It should be expected that attackers are monitoring all participants in the pipeline for possible weaknesses and standard security practices will address these needs. Security risks unique to WEA may not be fully addressed by standard security practices.
4. Some of these threat vectors described require a compromise of the CMSP network infrastructure. While in theory, such vulnerability may exist, it is not clear that a malicious actor would really spend their time, money, and other resources to breach the CMSP network to get to WEA or use the breach for access to subscriber confidential information or perform other actions which may have a financial value or more significant effect.
5. Some of the threat vectors have the unwritten assumption that WEA would be the sole source of alert information in order for the DoS attack to be effective. If such severe threat to life or property is imminent, the alert will be distributed via all available methods including radio, TV, highway message boards, sirens, loud speakers on police vehicles, etc. The DoS attack on WEA would be ineffective for the objective of not informing the public.
6. WEA is not the only source of information. Crowd behavior is another non-technical reaction. If everybody is running away from a building, you are not going to wait for a WEA message before deciding whether or not you are going to leave the area of the building.

## Recommendations

It is WG2’s recommendation that the FCC collaborate with industry, FEMA, DHS, and the Alert Originators to continue the study of the security aspects of WEA, with a goal of encouraging ATIS to develop a Best Practices document. The development of such a best practices document will require extensive work of more than a year, which would extend beyond the current CSRIC charter. WG2 Recommends that the FCC should consider asking any subsequent CSRIC to continue the study of WEA security based on this work.

Following is a list a general recommendations to mitigate the security risks that were highlighted in this Report:

* As the largest single risk to the WEA system is for a disgruntled alert originator to send a false message, it is recommended that all persons with credentials that allow them to create and send a WEA alert should undergo appropriate training, evaluations and background checks once per year in order to maintain such credentials.
* In order to mitigate the risks associated with malicious code in a supply chain vendor product, it is recommended that the WEA element containing the malicious software is taken offline immediately when found to contain malicious code that results in a false WEA alert or that suppresses a proper WEA alert.
* In order to mitigate the risks associated with a warning app that effectively mimics the look and sound of a WEA alert on a user’s device used for malicious intent, it is recommended that app store providers establish a procedure to identify and disallow such apps from inclusion in their online app stores. However, the following questions require further consideration:
  + What if the malicious warning app is hidden in a valid program?
  + What if the malicious warning app was not downloaded from an app store?
  + What if the malicious warning app had been downloaded from an app store before it was detected? The app store could remove it from further downloads but what about the devices which already have the malicious warning app installed?

It is recommended that the industry, FEMA, DHS, and Alert Originators collaborate on the development a new Best Practices standard in ATIS which includes:

* Security vulnerability and penetration test cases.
* Consideration for security event monitoring, such as Log monitoring, event correlation, and analysis as well as; DDoS protection, which will help strengthening the tracking capability for verification of expected alerts as they flow through the pipeline to provide an additional means for readily identifying false alerts.
* Consideration for identity and access management. Examples include: access administration, two-factor authentication, and federation and credential services covering all transaction in the WEA ecosystem.

To address the issue of protocol vulnerability, it recommended that the industry, FEMA, and the Alert Originators investigate existing protocol security vulnerability documented today with the aim of ensuring that all WEA related systems and specifications are up to date.

# Conclusions

Based on the WEA security analysis conducted in Working Group 2, it is our conclusion that the additional security measures as described in the Recommendation section of this report may mitigate security threats identified in this report. To that end, it is recommended that the industry, FEMA, DHS, and Alert Originators collaborate on the development a new Best Practices standard in ATIS.

# Appendix A: Acronyms

This Appendix contains the acronyms that are referenced within this report.

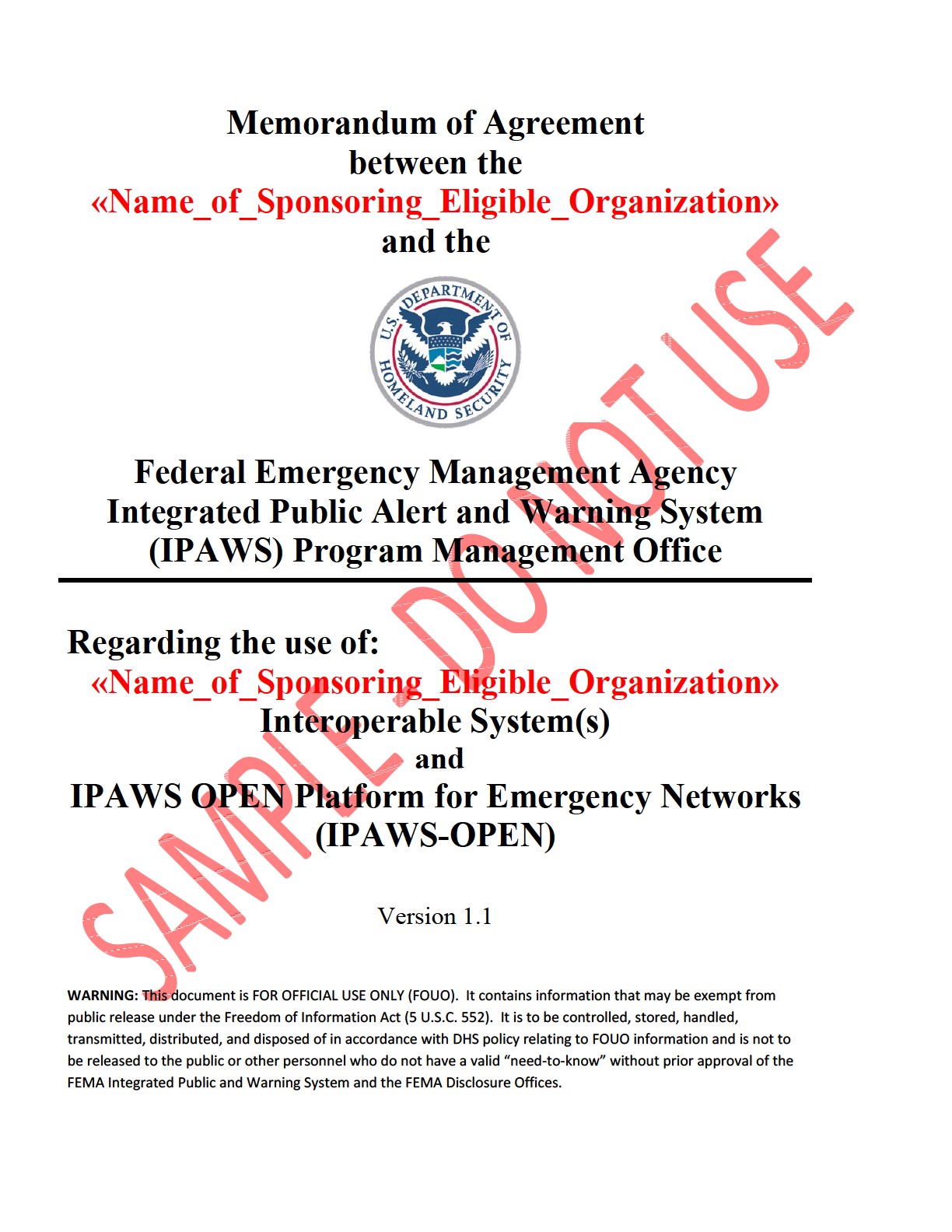
| Acronym | Definition | |
| --- | --- | --- |
| 3GPP | 3rd Generation Partner Project | |
| 4G | Fourth Generation | |
| ATIS | Alliance for Telecommunications Industry Solutions | |
| AO | Alert Originator | |
| CAP | Common Alerting Protocol |
| CDMA | Code Division Multiple Access |
| CFR | Code of Federal Regulations |
| CMAS | Commercial Mobile Alert Service |
| CMS | Commercial Mobile Service |
| CMSP | Commercial Mobile Service Provider |
| CSRIC | Communications Security, Reliability and Interoperability Council |
| DDoS | Distributed Denial of Service |
| DHS | Department of Homeland Security |
| DHS S&T | Department of Homeland Security Science and Technology Directorate |
| DNS | Domain Name System (Server) |
| DoS | Denial of Service |
| EIA | Electronic Industries Alliance |
| FCC | Federal Communications Commission |
| FEMA | Federal Emergency Management Agency |
| FIPS | Federal Information Processing Standard |
| GPS | Global Positioning System |
| IPAWS | Integrated Public Alert and Warning System |
| LTE | Long Term Evolution |
| MOA | Memorandum of Agreement |
| NIST | National Institute of Standards and Technology |
| NOAA | National Oceanic and Atmospheric Administration |
| NWS | National Weather Service |
| OASIS | Organization for the Advancement of Structured Information Standards |
| PTV | Public Television |
| PWS | Public Warning System |
| RAN | Radio Access Network |
| RF | Radio Frequency |
| SWG | Sub-Working Group |
| TCP | Transmission Control Protocol |
| TIA | Telecommunications Industry Association |
| TIC | Trusted Internet Connection |
| URL | Uniform Resource Locator |
| WARN | Warning, Alert, and Response Network |
| WEA | Wireless Emergency Alerts |

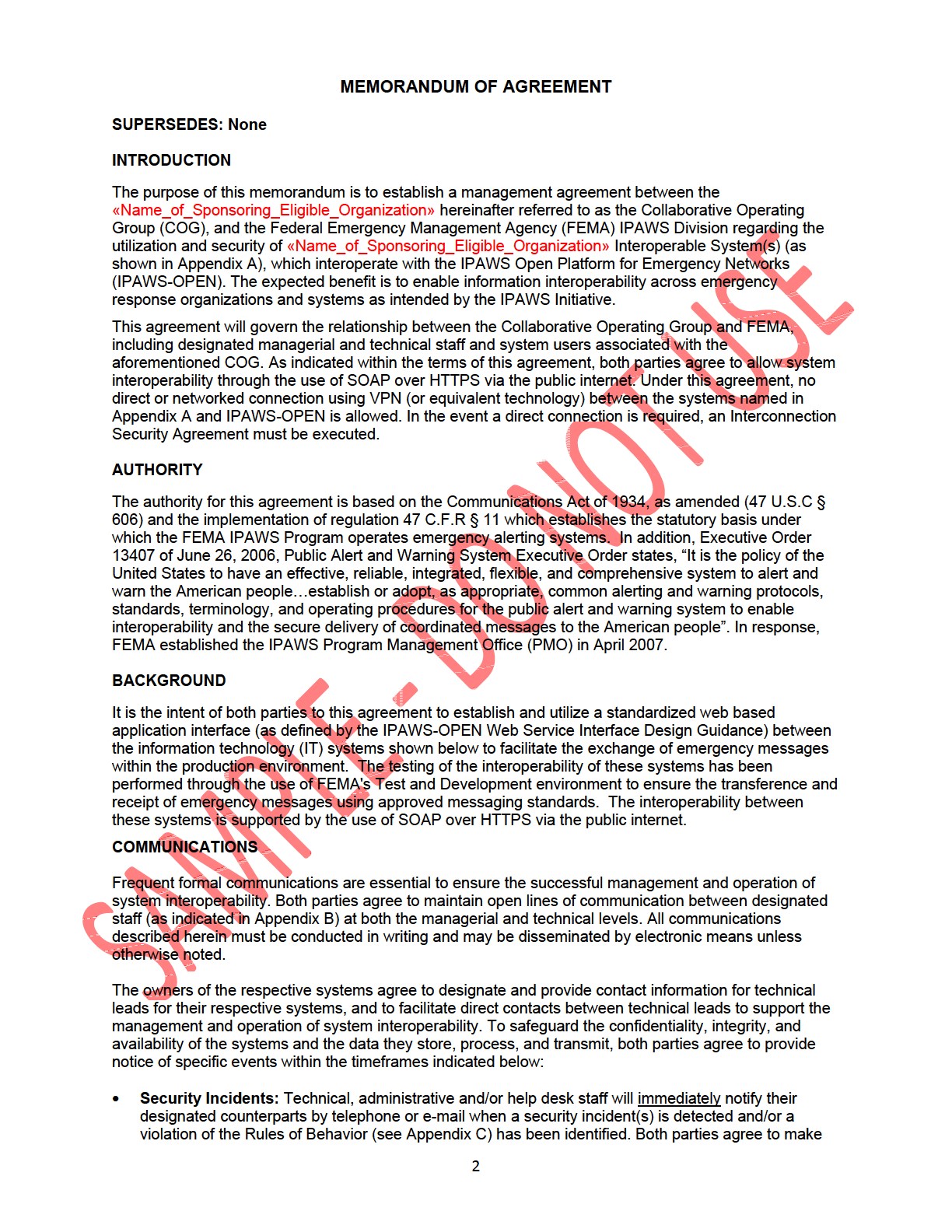
# Appendix B: Glossary

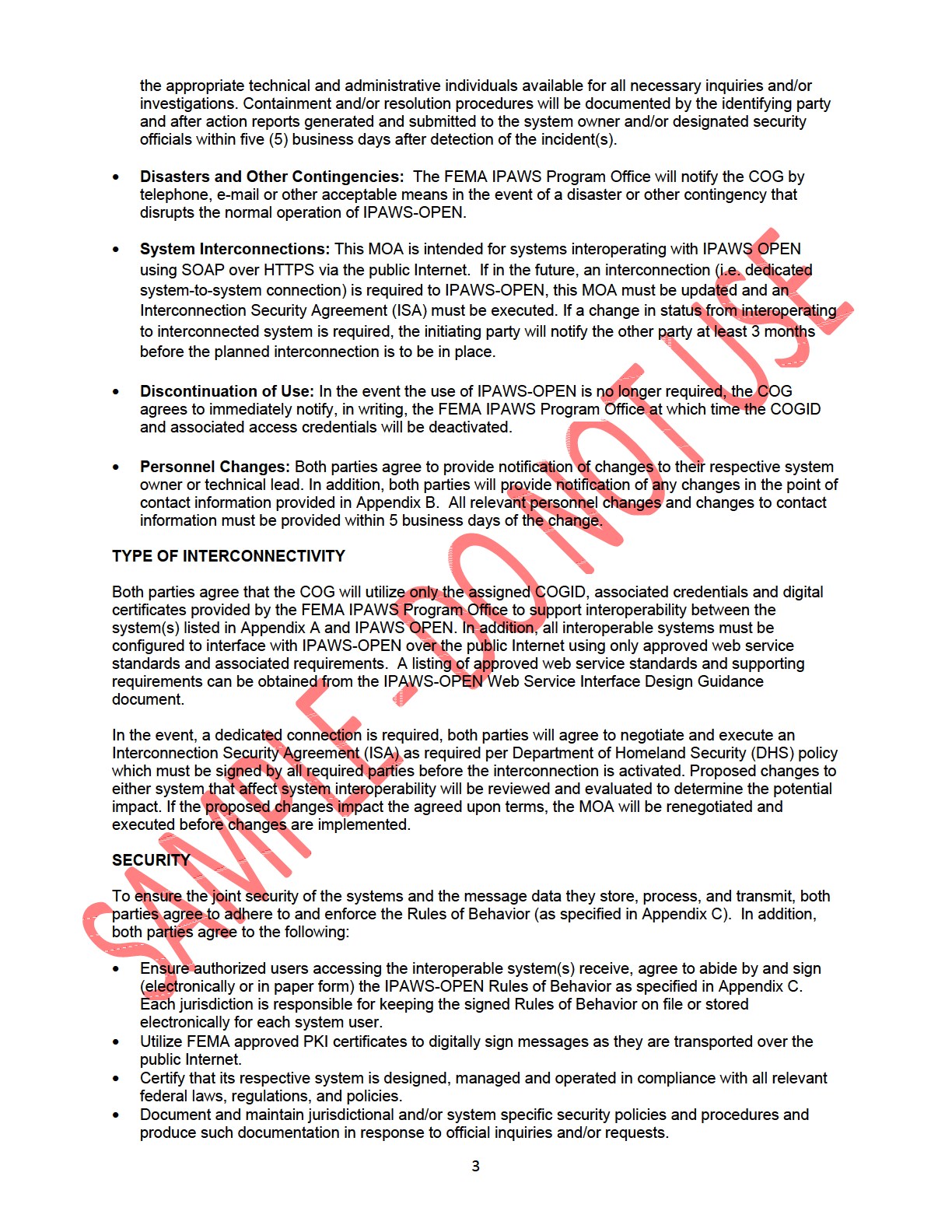
This Appendix contains the glossary associated with this report.

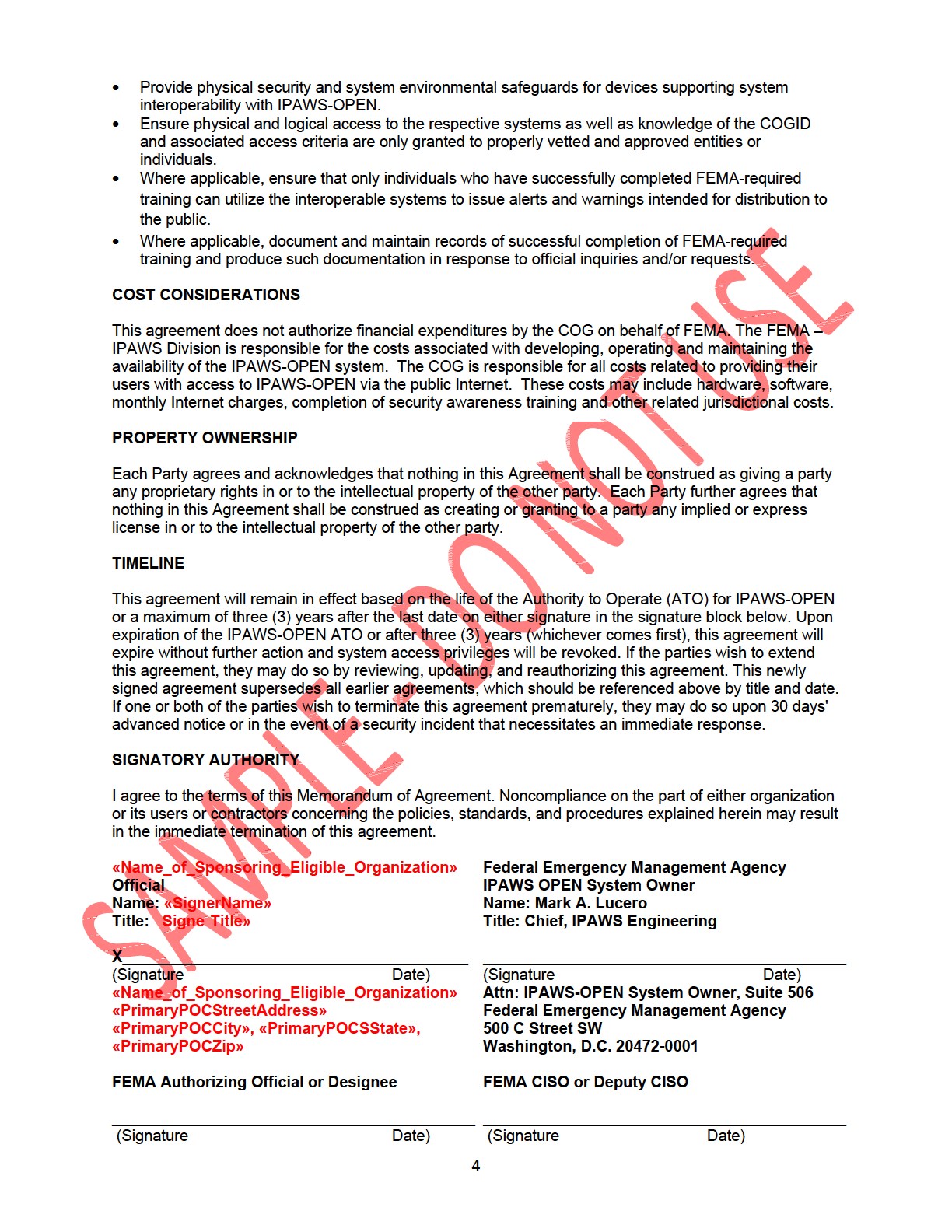
| Term | Definition |
| --- | --- |
| 3GPP | The 3rd Generation Partnership Project (3GPP) is a collaboration agreement that was established in December 1998.  The collaboration agreement brings together a number of telecommunications standards bodies which are known as “Organizational Partners”. |
| Access Provider | An access provider is any organization that arranges for an individual or an organization to have access to the Internet. |
| Alliance for Telecommunications Industry Solutions (ATIS) | A U.S.-based organization that is committed to rapidly developing and promoting technical and operations standards for the communications and related information technologies industry worldwide using a pragmatic, flexible and open approach. <http://www.atis.org/> |
| Department of Homeland Security (DHS) | Department of the Federal Government with five homeland security missions. These missions include preventing terrorism and enhancing security, securing and managing U.S. borders, enforcing and administering U.S. immigration laws, safeguarding and securing cyberspace, and ensuring resilience to disasters. |
| Geocoding | Translation of one form of location into another, typically a civic address into an x, y coordinate. |
| Geo Location | Latitude, longitude, elevation, and the datum which identifies the coordinate system used. |
| Geographic Targeting  (geo-targeting) | The 47 CFR Part 10, Subpart D - Alert Message Requirements defines geographic targeting (geo-targeting) as follows:  “§ 10.450 Geographic targeting.  This section establishes minimum requirements for the geographic targeting of Alert Messages. A Participating CMS Provider will determine which of its network facilities, elements, and locations will be used to geographically target Alert Messages. A Participating CMS Provider must transmit any Alert Message that is specified by a geocode, circle, or polygon to an area not larger than the provider's approximation of coverage for the Counties or County Equivalents with which that geocode, circle, or polygon intersects. If, however, the propagation area of a provider's transmission site exceeds a single County or County Equivalent, a Participating CMS Provider may transmit an Alert Message to an area not exceeding the propagation area.” |
| Geospatial | Data accurately referenced to a precise location on the earth’s surface. |
| Global Positioning System (GPS) | A satellite based Location Determination Technology (LDT). |
| Spatial | Relating to, occupying, or having the character of space. Geographic Information Systems store spatial data in regional databases. See Geospatial. |
| Wireless Industry | Mobile Network operators and their equipment vendors (including device OEMs and OS implementers) who plan, standardize, develop, implement and maintain the commercial cellular mobile networks and devices. |
| Working Group (WG) | A group of people formed to discuss and develop a response to a particular issue. The response may result in a Standard, an Information Document, Technical Requirements Document or Liaison. |
| X,y | Shorthand expression for coordinates that identify a specific location in two dimensions representing latitude and longitude. |

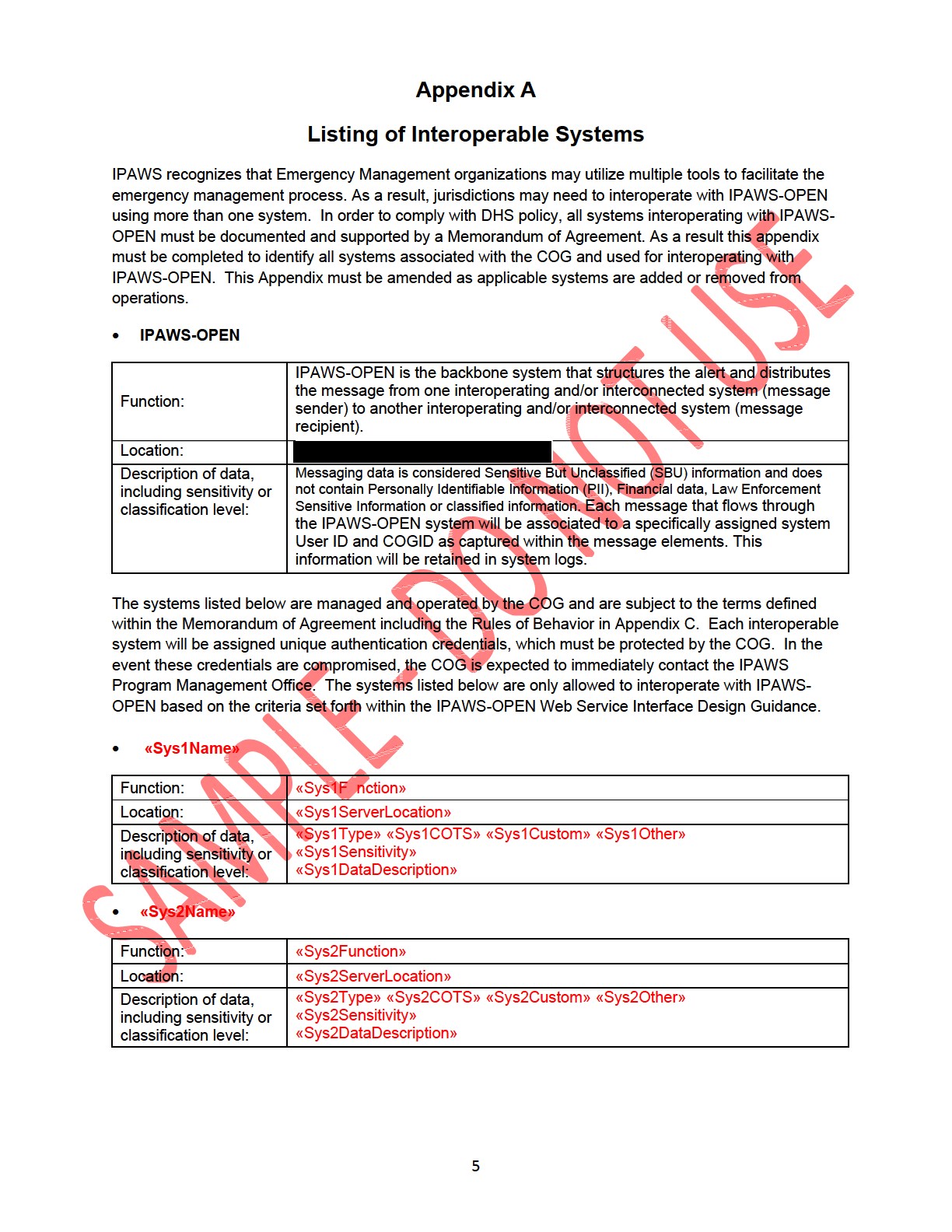
# Appendix C: Sample MOA – Between FEMA & Alert Originators

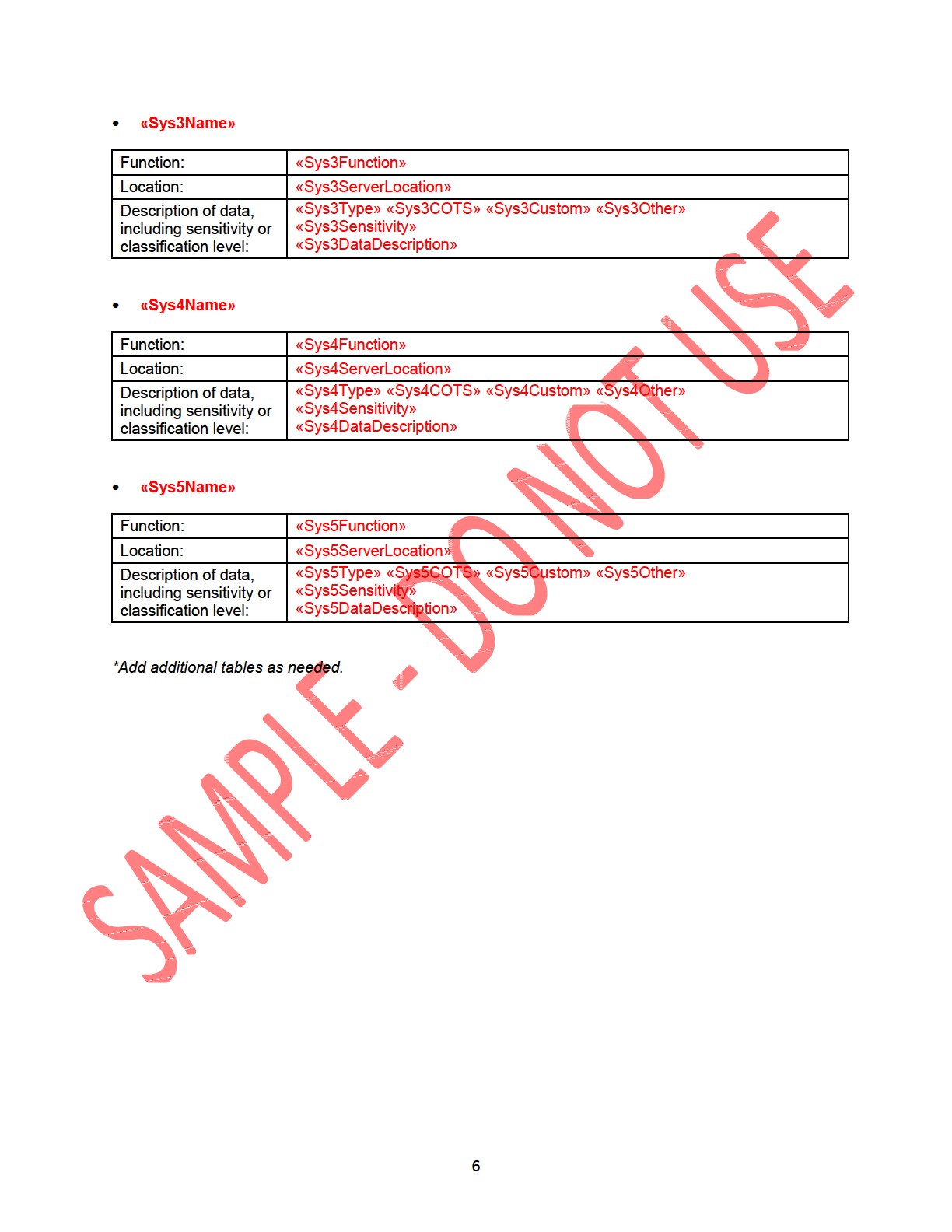




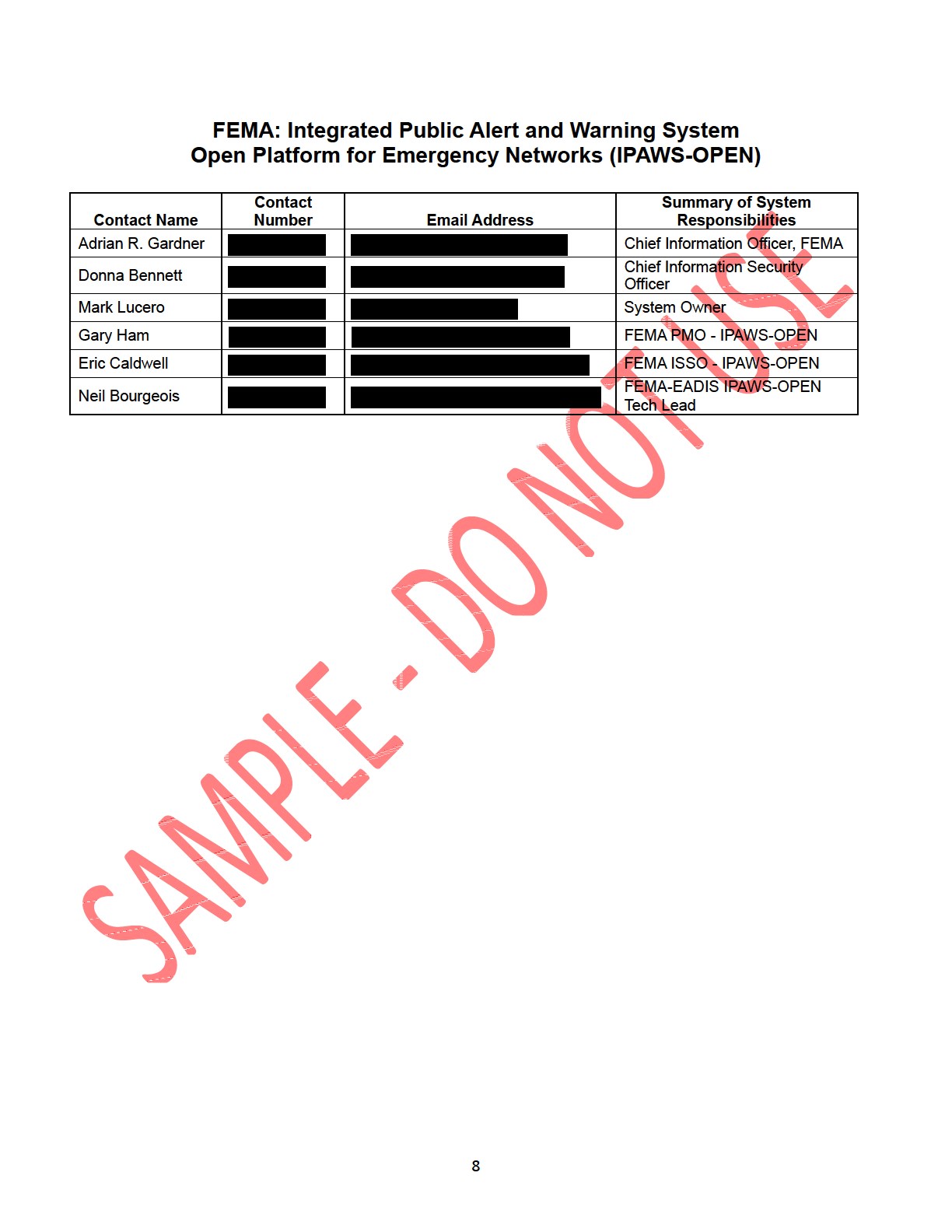


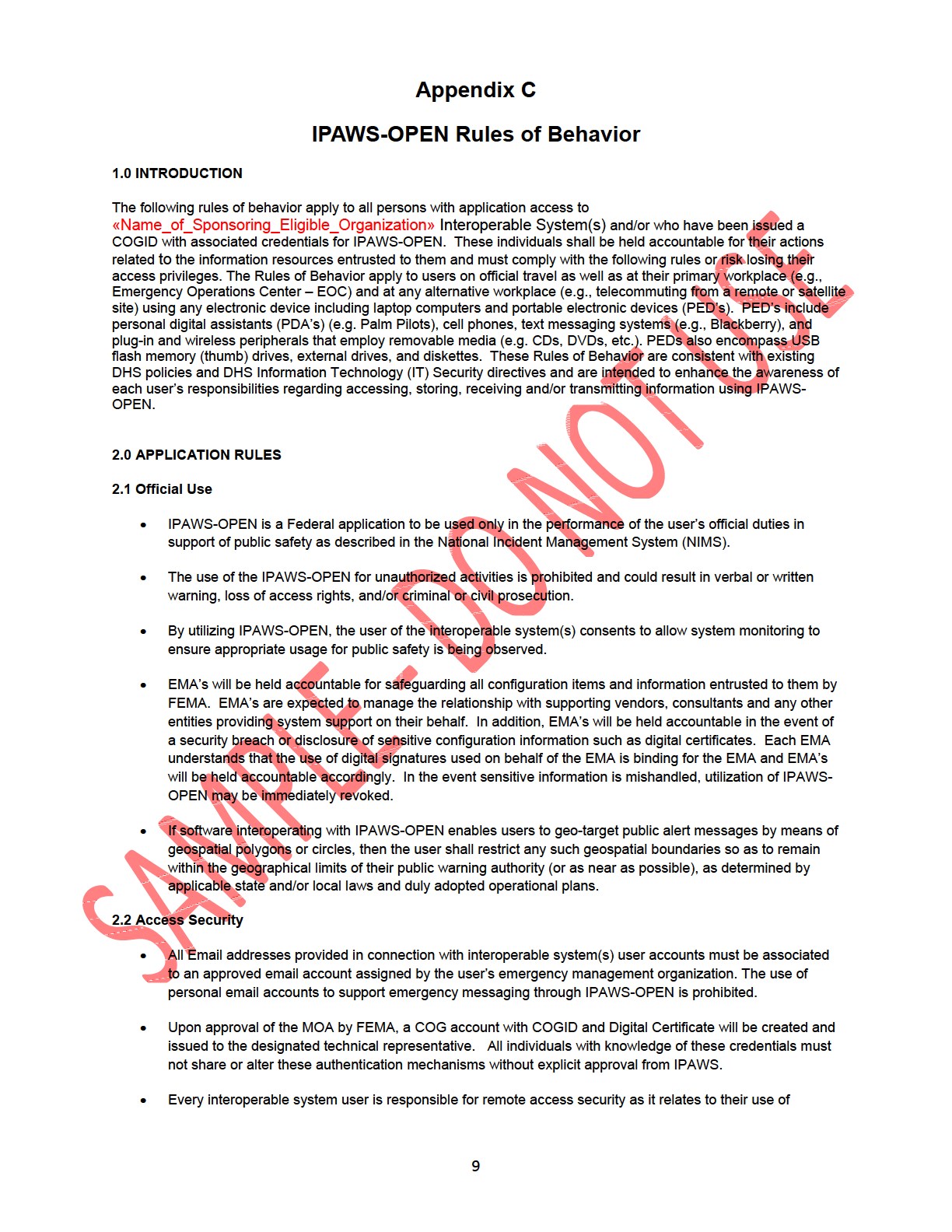


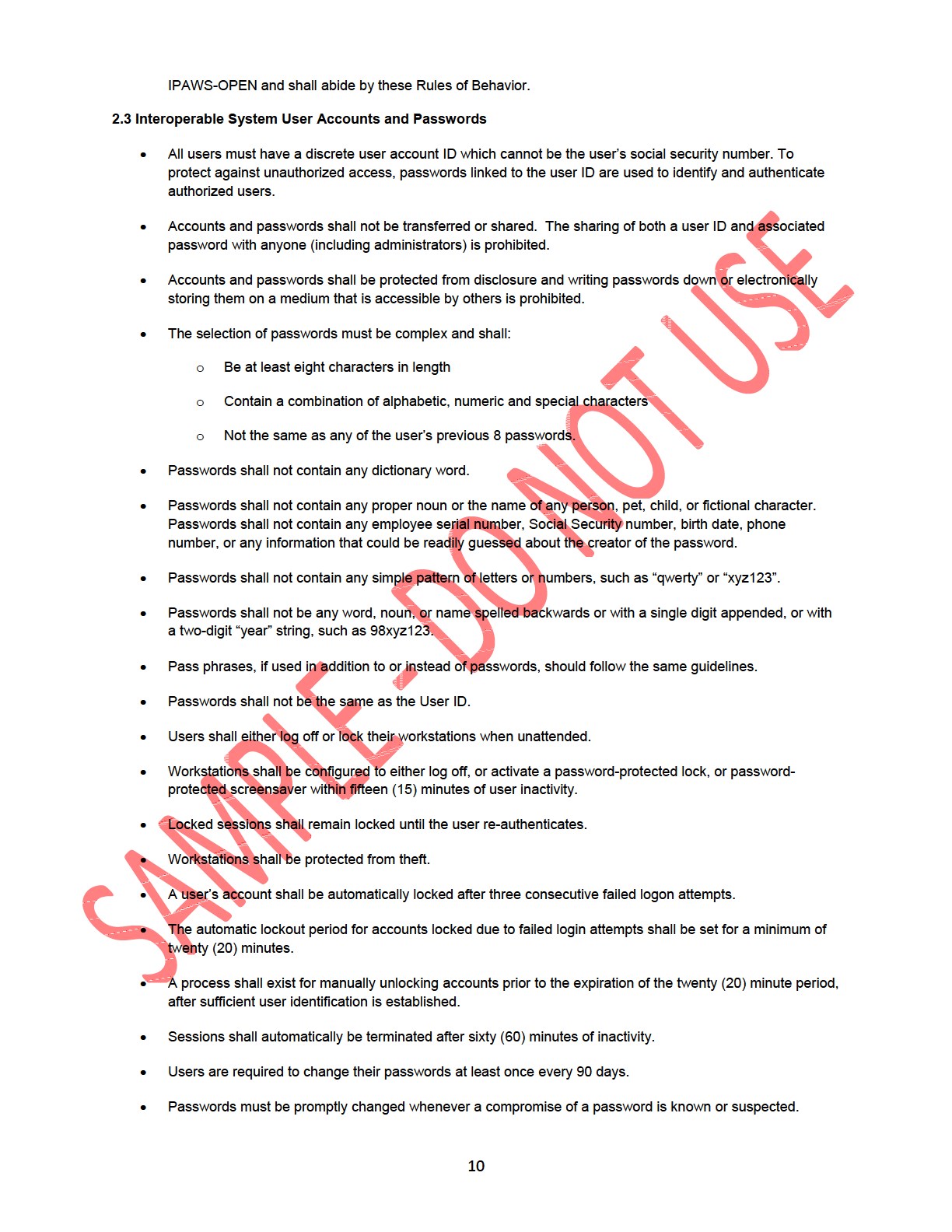


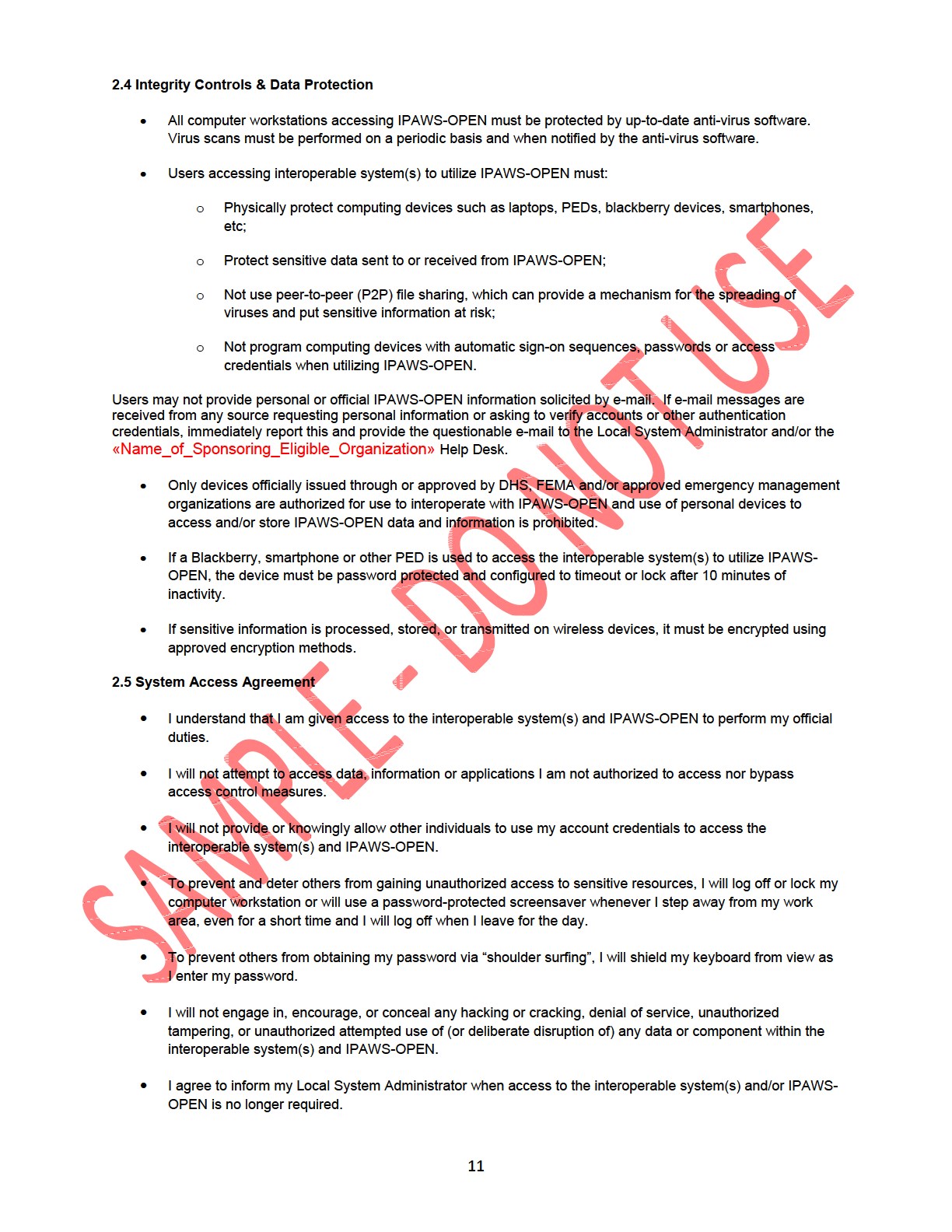


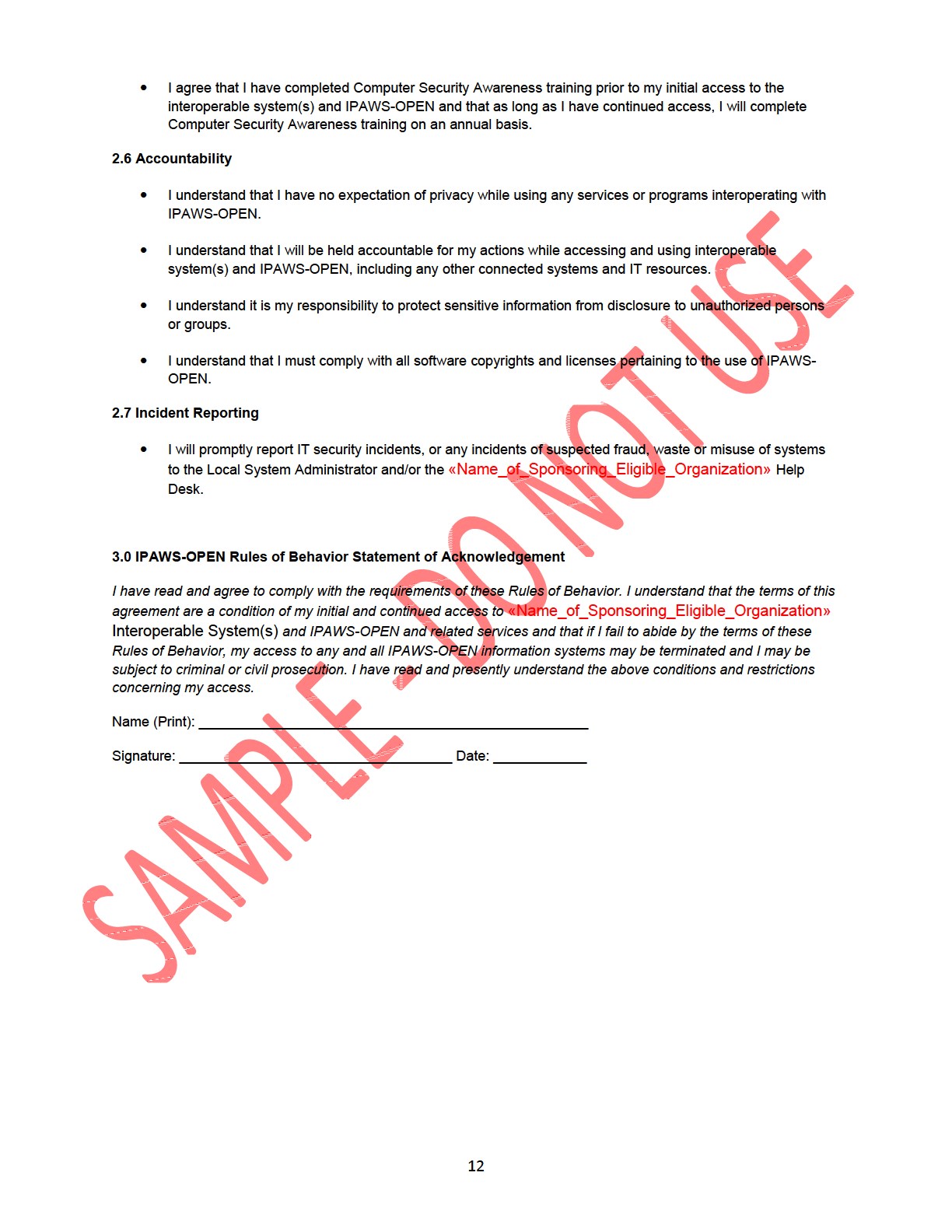












1. The FCC approved a Notice of Proposed Rulemaking to Improve Wireless Emergency Alerts and Community-Initiated Alerting, PS Docket No. 15-91, in November 2015. [↑](#footnote-ref-1)
2. This document is available from the Federal Communications Commission. <<http://www.fcc.gov/>> [↑](#footnote-ref-2)
3. This document is available from the Organization for the Advancement of Structured Information Standards (OASIS).  
    <<http://www.oasis-open.org/specs/index.php>> [↑](#footnote-ref-3)
4. This document is available from the Alliance for Telecommunications Industry Solutions (ATIS) < <http://www.atis.org> > [↑](#footnote-ref-4)
5. This document is available from <http://www.firstresponder.gov/SitePages/SiteSearch/SiteSearch.aspx?k=WEA> [↑](#footnote-ref-5)
6. This document is available from< http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf> [↑](#footnote-ref-6)
7. This document is available from < <http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf>> [↑](#footnote-ref-7)
8. This document is available from <http://dx.doi.org/10.6028/NIST.SP.800-37r1> [↑](#footnote-ref-8)
9. This document is available from < http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf> [↑](#footnote-ref-9)
10. This document is available from < http://dx.doi.org/10.6028/NIST.SP.800-53r4> [↑](#footnote-ref-10)
11. This document is available from < https://www.dhs.gov/xlibrary/assets/foia/mgmt\_directive\_4300a\_policy\_v8.pdf> [↑](#footnote-ref-11)
12. This document is available from < http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf> [↑](#footnote-ref-12)
13. This document is available from the Third Generation Partnership Project (3GPP) at   
    < <http://www.3gpp.org/specs/specs.htm> > [↑](#footnote-ref-13)
14. www.nist.gov/cyberframework [↑](#footnote-ref-14)
15. Industry standard documents, such as ATIS J-STD-101 [Ref 19] , refer to the PBS WARN system to as the “C-OTA Interface” [↑](#footnote-ref-15)
16. PBS Technical Specification PWS-005 [↑](#footnote-ref-16)