# Memorandum of Agreement
# between the
# Gallatin County Emergency Management
# and the

# Federal Emergency Management Agency
# Integrated Public Alert and Warning System
# (IPAWS) Program Management Office

---

# Regarding the use of:
# Gallatin County Emergency Management
# Interoperable System(s)
# and
# IPAWS OPEN Platform for Emergency Networks
# (IPAWS-OPEN)

Version 1.1

April 17, 2015

**WARNING:** This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of the FEMA Integrated Public and Warning System and the FEMA Disclosure Offices.

## MEMORANDUM OF AGREEMENT

**SUPERSEDES: None**

### INTRODUCTION

The purpose of this memorandum is to establish a management agreement between the Gallatin County Emergency Management hereinafter referred to as the Collaborative Operating Group (COG), and the Federal Emergency Management Agency (FEMA) IPAWS Division regarding the utilization and security of Gallatin County Emergency Management Interoperable System(s) (as shown in Appendix A), which interoperate with the IPAWS Open Platform for Emergency Networks (IPAWS-OPEN). The expected benefit is to enable information interoperability across emergency response organizations and systems as intended by the IPAWS Initiative.

This agreement will govern the relationship between the Collaborative Operating Group and FEMA, including designated managerial and technical staff and system users associated with the aforementioned COG. As indicated within the terms of this agreement, both parties agree to allow system interoperability through the use of SOAP over HTTPS via the public internet. Under this agreement, no direct or networked connection using VPN (or equivalent technology) between the systems named in Appendix A and IPAWS-OPEN is allowed. In the event a direct connection is required, an Interconnection Security Agreement must be executed.

### AUTHORITY

The authority for this agreement is based on the Communications Act of 1934, as amended (47 U.S.C § 606) and the implementation of regulation 47 C.F.R § 11 which establishes the statutory basis under which the FEMA IPAWS Program operates emergency alerting systems. In addition, Executive Order 13407 of June 26, 2006, Public Alert and Warning System Executive Order states, "It is the policy of the United States to have an effective, reliable, integrated, flexible, and comprehensive system to alert and warn the American people...establish or adopt, as appropriate, common alerting and warning protocols, standards, terminology, and operating procedures for the public alert and warning system to enable interoperability and the secure delivery of coordinated messages to the American people". In response, FEMA established the IPAWS Program Management Office (PMO) in April 2007.

### BACKGROUND

It is the intent of both parties to this agreement to establish and utilize a standardized web based application interface (as defined by the IPAWS-OPEN Web Service Interface Design Guidance) between the information technology (IT) systems shown below to facilitate the exchange of emergency messages within the production environment. The testing of the interoperability of these systems has been performed through the use of FEMA's Test and Development environment to ensure the transference and receipt of emergency messages using approved messaging standards. The interoperability between these systems is supported by the use of SOAP over HTTPS via the public internet.

### COMMUNICATIONS

Frequent formal communications are essential to ensure the successful management and operation of system interoperability. Both parties agree to maintain open lines of communication between designated staff (as indicated in Appendix B) at both the managerial and technical levels. All communications described herein must be conducted in writing and may be disseminated by electronic means unless otherwise noted.

The owners of the respective systems agree to designate and provide contact information for technical leads for their respective systems, and to facilitate direct contacts between technical leads to support the management and operation of system interoperability. To safeguard the confidentiality, integrity, and availability of the systems and the data they store, process, and transmit, both parties agree to provide notice of specific events within the timeframes indicated below:

- **Security Incidents:** Technical, administrative and/or help desk staff will immediately notify their designated counterparts by telephone or e-mail when a security incident(s) is detected and/or a violation of the Rules of Behavior (see Appendix C) has been identified. Both parties agree to make the appropriate technical and administrative individuals available for all necessary inquiries and/or

investigations. Containment and/or resolution procedures will be documented by the identifying party and after action reports generated and submitted to the system owner and/or designated security officials within five (5) business days after detection of the incident(s).

- **Disasters and Other Contingencies:** The FEMA IPAWS Program Office will notify the COG by telephone, e-mail or other acceptable means in the event of a disaster or other contingency that disrupts the normal operation of IPAWS-OPEN.

- **System Interconnections:** This MOA is intended for systems interoperating with IPAWS OPEN using SOAP over HTTPS via the public Internet. If in the future, an interconnection (i.e. dedicated system-to-system connection) is required to IPAWS-OPEN, this MOA must be updated and an Interconnection Security Agreement (ISA) must be executed. If a change in status from interoperating to interconnected system is required, the initiating party will notify the other party at least 3 months before the planned interconnection is to be in place.

- **Discontinuation of Use:** In the event the use of IPAWS-OPEN is no longer required, the COG agrees to immediately notify, in writing, the FEMA IPAWS Program Office at which time the COGID and associated access credentials will be deactivated.

- **Personnel Changes:** Both parties agree to provide notification of changes to their respective system owner or technical lead. In addition, both parties will provide notification of any changes in the point of contact information provided in Appendix B. All relevant personnel changes and changes to contact information must be provided within 5 business days of the change.

**TYPE OF INTERCONNECTIVITY**

Both parties agree that the COG will utilize only the assigned COGID, associated credentials and digital certificates provided by the FEMA IPAWS Program Office to support interoperability between the system(s) listed in Appendix A and IPAWS OPEN. In addition, all interoperable systems must be configured to interface with IPAWS-OPEN over the public Internet using only approved web service standards and associated requirements. A listing of approved web service standards and supporting requirements can be obtained from the IPAWS-OPEN Web Service Interface Design Guidance document.

In the event, a dedicated connection is required, both parties will agree to negotiate and execute an Interconnection Security Agreement (ISA) as required per Department of Homeland Security (DHS) policy which must be signed by all required parties before the interconnection is activated. Proposed changes to either system that affect system interoperability will be reviewed and evaluated to determine the potential impact. If the proposed changes impact the agreed upon terms, the MOA will be renegotiated and executed before changes are implemented.

**SECURITY**

To ensure the joint security of the systems and the message data they store, process, and transmit, both parties agree to adhere to and enforce the Rules of Behavior (as specified in Appendix C). In addition, both parties agree to the following:

- Ensure authorized users accessing the interoperable system(s) receive, agree to abide by and sign (electronically or in paper form) the IPAWS-OPEN Rules of Behavior as specified in Appendix C. Each jurisdiction is responsible for keeping the signed Rules of Behavior on file or stored electronically for each system user.
- Utilize FEMA approved PKI certificates to digitally sign messages as they are transported over the public Internet.
- Certify that its respective system is designed, managed and operated in compliance with all relevant federal laws, regulations, and policies.
- Document and maintain jurisdictional and/or system specific security policies and procedures and produce such documentation in response to official inquiries and/or requests.
- Provide physical security and system environmental safeguards for devices supporting system interoperability with IPAWS-OPEN.

- Ensure physical and logical access to the respective systems as well as knowledge of the COGID and associated access criteria are only granted to properly vetted and approved entities or individuals.
- Where applicable, ensure that only individuals who have successfully completed FEMA-required training can utilize the interoperable systems to issue alerts and warnings intended for distribution to the public.
- Where applicable, document and maintain records of successful completion of FEMA-required training and produce such documentation in response to official inquiries and/or requests.

**COST CONSIDERATIONS**

This agreement does not authorize financial expenditures by the COG on behalf of FEMA. The FEMA – IPAWS Division is responsible for the costs associated with developing, operating and maintaining the availability of the IPAWS-OPEN system. The COG is responsible for all costs related to providing their users with access to IPAWS-OPEN via the public Internet. These costs may include hardware, software, monthly Internet charges, completion of security awareness training and other related jurisdictional costs.

**PROPERTY OWNERSHIP**

Each Party agrees and acknowledges that nothing in this Agreement shall be construed as giving a party any proprietary rights in or to the intellectual property of the other party. Each Party further agrees that nothing in this Agreement shall be construed as creating or granting to a party any implied or express license in or to the intellectual property of the other party.

**TIMELINE**

This agreement will remain in effect based on the life of the Authority to Operate (ATO) for IPAWS-OPEN or a maximum of three (3) years after the last date on either signature in the signature block below. Upon expiration of the IPAWS-OPEN ATO or after three (3) years (whichever comes first), this agreement will expire without further action and system access privileges will be revoked. If the parties wish to extend this agreement, they may do so by reviewing, updating, and reauthorizing this agreement. This newly signed agreement supersedes all earlier agreements, which should be referenced above by title and date. If one or both of the parties wish to terminate this agreement prematurely, they may do so upon 30 days' advanced notice or in the event of a security incident that necessitates an immediate response.

**SIGNATORY AUTHORITY**

I agree to the terms of this Memorandum of Agreement. Noncompliance on the part of either organization or its users or contractors concerning the policies, standards, and procedures explained herein may result in the immediate termination of this agreement.

**Gallatin County Emergency Management Official**
**Name: Steve White**
**Title: Chairman, Board of Commissioners**

X _____ 6-2-15
(Signature Date)

**Gallatin County Emergency Management**
**34 N Rouse Avenue**
**Bozeman, MT 59715**

**Federal Emergency Management Agency**
**IPAWS OPEN System Owner**
**Name: Mark A. Lucero**
**Title: Chief, IPAWS Engineering**

MARK A LUCERO Digitally signed by MARK A LUCERO DN: c=US, o=U.S. Government, ou=Department of Homeland Security, ou=FEMA, ou=People, cn=MARK A LUCERO, 0.9.2342.19200300.100.1.1=0623735800 FEMA Date: 2015.06.09 11:57:31 -04'00'

(Signature Date)

**Attn: IPAWS-OPEN System Owner, Suite 506**
**Federal Emergency Management Agency**
**500 C Street SW**
**Washington, D.C. 20472-0001**

**FEMA Authorizing Official or Designee**

(Signature Date)

**FEMA CISO or Deputy CISO**

(Signature Date)

# Appendix A

## Listing of Interoperable Systems

IPAWS recognizes that Emergency Management organizations may utilize multiple tools to facilitate the emergency management process. As a result, jurisdictions may need to interoperate with IPAWS-OPEN using more than one system. In order to comply with DHS policy, all systems interoperating with IPAWS-OPEN must be documented and supported by a Memorandum of Agreement. As a result this appendix must be completed to identify all systems associated with the COG and used for interoperating with IPAWS-OPEN. This Appendix must be amended as applicable systems are added or removed from operations.

- **IPAWS-OPEN**

| | |
|---|---|
| Function: | IPAWS-OPEN is the backbone system that structures the alert and distributes the message from one interoperating and/or interconnected system (message sender) to another interoperating and/or interconnected system (message recipient). |
| Location: | FEMA Emergency Operations Center |
| Description of data, including sensitivity or classification level: | Messaging data is considered Sensitive But Unclassified (SBU) information and does not contain Personally Identifiable Information (PII), Financial data, Law Enforcement Sensitive Information or classified information. Each message that flows through the IPAWS-OPEN system will be associated to a specifically assigned system User ID and COGID as captured within the message elements. This information will be retained in system logs. |

The systems listed below are managed and operated by the COG and are subject to the terms defined within the Memorandum of Agreement including the Rules of Behavior in Appendix C. Each interoperable system will be assigned unique authentication credentials, which must be protected by the COG. In the event these credentials are compromised, the COG is expected to immediately contact the IPAWS Program Management Office. The systems listed below are only allowed to interoperate with IPAWS-OPEN based on the criteria set forth within the IPAWS-OPEN Web Service Interface Design Guidance.

- **Everbridge Aware, Everbridge Matrix, Everbridge SmartGIS, Everbridge Mass Notification, Everbridge Interactive Visibility**

| | |
|---|---|
| Function: | Send public alerts for major events for dissemination to WEA |
| Location: | Burbank, CA; Denver, CO; Amazon West Northern, CA |
| Description of data, including sensitivity or classification level: | COTS<br>FOUO<br>Data is comprised of emergency public alert messages |

**Add additional tables as needed.*

# Appendix B

## COG Point of Contact Information

### Designated COG Primary Point of Contact:

**Name: Patrick Lonergan**

**Title: Director**

**Business Email Address:** [redacted]

**Primary Phone Number: 4**[redacted]

**Alternate Phone Number:**

**Organization: Gallatin County Emergency Management**

**Mailing Address: 34 N Rouse Avenue, Bozeman, MT 59715**

### Designated Alternate Point of Contact:

**Name: Bruce Cunningham**

**Title: CAD Administrator**

**Business Email Address** [redacted]

**Primary Phone Number:**

**Alternate Phone Number:**

**Organization: Gallatin County 911**

**Mailing Address: 1705 Vaquero, Bozeman, MT 59715**

### Designated Technical Point of Contact:

**Name: Patrick Lonergan**

**Title: Director**

**Business Email Address:** [redacted]

**Primary Phone Number: 4**[redacted]

**Alternate Phone Number:**

**Organization: Gallatin County Emergency Management**

**Mailing Address: 34 N Rouse Avenue, Bozeman, MT 59715**

# FEMA: Integrated Public Alert and Warning System Open Platform for Emergency Networks (IPAWS-OPEN)

| Contact Name | Contact Number | Email Address | Summary of System Responsibilities |
|---|---|---|---|
| Adrian R. Gardner | [redacted] | | Chief Information Officer, FEMA |
| Donna Bennett | | | Chief Information Security Officer |
| Mark Lucero | | | System Owner |
| Gary Ham | | | FEMA PMO - IPAWS-OPEN |
| Eric Caldwell | | | FEMA ISSO - IPAWS-OPEN |
| Neil Bourgeois | | | FEMA-EADIS IPAWS-OPEN Tech Lead |

# Appendix C

# IPAWS-OPEN Rules of Behavior

### 1.0 INTRODUCTION

The following rules of behavior apply to all persons with application access to Gallatin County Emergency Management Interoperable System(s) and/or who have been issued a COGID with associated credentials for IPAWS-OPEN. These individuals shall be held accountable for their actions related to the information resources entrusted to them and must comply with the following rules or risk losing their access privileges. The Rules of Behavior apply to users on official travel as well as at their primary workplace (e.g., Emergency Operations Center – EOC) and at any alternative workplace (e.g., telecommuting from a remote or satellite site) using any electronic device including laptop computers and portable electronic devices (PED's). PED's include personal digital assistants (PDA's) (e.g. Palm Pilots), cell phones, text messaging systems (e.g., Blackberry), and plug-in and wireless peripherals that employ removable media (e.g. CDs, DVDs, etc.). PEDs also encompass USB flash memory (thumb) drives, external drives, and diskettes. These Rules of Behavior are consistent with existing DHS policies and DHS Information Technology (IT) Security directives and are intended to enhance the awareness of each user's responsibilities regarding accessing, storing, receiving and/or transmitting information using IPAWS-OPEN.

### 2.0 APPLICATION RULES

#### 2.1 Official Use

- IPAWS-OPEN is a Federal application to be used only in the performance of the user's official duties in support of public safety as described in the National Incident Management System (NIMS).
- The use of the IPAWS-OPEN for unauthorized activities is prohibited and could result in verbal or written warning, loss of access rights, and/or criminal or civil prosecution.
- By utilizing IPAWS-OPEN, the user of the interoperable system(s) consents to allow system monitoring to ensure appropriate usage for public safety is being observed.
- EMA's will be held accountable for safeguarding all configuration items and information entrusted to them by FEMA. EMA's are expected to manage the relationship with supporting vendors, consultants and any other entities providing system support on their behalf. In addition, EMA's will be held accountable in the event of a security breach or disclosure of sensitive configuration information such as digital certificates. Each EMA understands that the use of digital signatures used on behalf of the EMA is binding for the EMA and EMA's will be held accountable accordingly. In the event sensitive information is mishandled, utilization of IPAWS-OPEN may be immediately revoked.
- If software interoperating with IPAWS-OPEN enables users to geo-target public alert messages by means of geospatial polygons or circles, then the user shall restrict any such geospatial boundaries so as to remain within the geographical limits of their public warning authority (or as near as possible), as determined by applicable state and/or local laws and duly adopted operational plans.

#### 2.2 Access Security

- All Email addresses provided in connection with interoperable system(s) user accounts must be associated to an approved email account assigned by the user's emergency management organization. The use of personal email accounts to support emergency messaging through IPAWS-OPEN is prohibited.
- Upon approval of the MOA by FEMA, a COG account with COGID and Digital Certificate will be created and issued to the designated technical representative. All individuals with knowledge of these credentials must not share or alter these authentication mechanisms without explicit approval from IPAWS.
- Every interoperable system user is responsible for remote access security as it relates to their use of IPAWS-OPEN and shall abide by these Rules of Behavior.

### 2.3 Interoperable System User Accounts and Passwords

- All users must have a discrete user account ID which cannot be the user's social security number. To protect against unauthorized access, passwords linked to the user ID are used to identify and authenticate authorized users.
- Accounts and passwords shall not be transferred or shared. The sharing of both a user ID and associated password with anyone (including administrators) is prohibited.
- Accounts and passwords shall be protected from disclosure and writing passwords down or electronically storing them on a medium that is accessible by others is prohibited.
- The selection of passwords must be complex and shall:
    - Be at least eight characters in length
    - Contain a combination of alphabetic, numeric and special characters
    - Not the same as any of the user's previous 8 passwords.
- Passwords shall not contain any dictionary word.
- Passwords shall not contain any proper noun or the name of any person, pet, child, or fictional character. Passwords shall not contain any employee serial number, Social Security number, birth date, phone number, or any information that could be readily guessed about the creator of the password.
- Passwords shall not contain any simple pattern of letters or numbers, such as “qwerty” or “xyz123”.
- Passwords shall not be any word, noun, or name spelled backwards or with a single digit appended, or with a two-digit “year” string, such as 98xyz123.
- Pass phrases, if used in addition to or instead of passwords, should follow the same guidelines.
- Passwords shall not be the same as the User ID.
- Users shall either log off or lock their workstations when unattended.
- Workstations shall be configured to either log off, or activate a password-protected lock, or password-protected screensaver within fifteen (15) minutes of user inactivity.
- Locked sessions shall remain locked until the user re-authenticates.
- Workstations shall be protected from theft.
- A user's account shall be automatically locked after three consecutive failed logon attempts.
- The automatic lockout period for accounts locked due to failed login attempts shall be set for a minimum of twenty (20) minutes.
- A process shall exist for manually unlocking accounts prior to the expiration of the twenty (20) minute period, after sufficient user identification is established.
- Sessions shall automatically be terminated after sixty (60) minutes of inactivity.
- Users are required to change their passwords at least once every 90 days.
- Passwords must be promptly changed whenever a compromise of a password is known or suspected.

### 2.4 Integrity Controls & Data Protection

- All computer workstations accessing IPAWS-OPEN must be protected by up-to-date anti-virus software. Virus scans must be performed on a periodic basis and when notified by the anti-virus software.

- Users accessing interoperable system(s) to utilize IPAWS-OPEN must:

    - Physically protect computing devices such as laptops, PEDs, blackberry devices, smartphones, etc;

    - Protect sensitive data sent to or received from IPAWS-OPEN;

    - Not use peer-to-peer (P2P) file sharing, which can provide a mechanism for the spreading of viruses and put sensitive information at risk;

    - Not program computing devices with automatic sign-on sequences, passwords or access credentials when utilizing IPAWS-OPEN.

Users may not provide personal or official IPAWS-OPEN information solicited by e-mail. If e-mail messages are received from any source requesting personal information or asking to verify accounts or other authentication credentials, immediately report this and provide the questionable e-mail to the Local System Administrator and/or the Gallatin County Emergency Management Help Desk.

- Only devices officially issued through or approved by DHS, FEMA and/or approved emergency management organizations are authorized for use to interoperate with IPAWS-OPEN and use of personal devices to access and/or store IPAWS-OPEN data and information is prohibited.

- If a Blackberry, smartphone or other PED is used to access the interoperable system(s) to utilize IPAWS-OPEN, the device must be password protected and configured to timeout or lock after 10 minutes of inactivity.

- If sensitive information is processed, stored, or transmitted on wireless devices, it must be encrypted using approved encryption methods.

**2.5 System Access Agreement**

- I understand that I am given access to the interoperable system(s) and IPAWS-OPEN to perform my official duties.

- I will not attempt to access data, information or applications I am not authorized to access nor bypass access control measures.

- I will not provide or knowingly allow other individuals to use my account credentials to access the interoperable system(s) and IPAWS-OPEN.

- To prevent and deter others from gaining unauthorized access to sensitive resources, I will log off or lock my computer workstation or will use a password-protected screensaver whenever I step away from my work area, even for a short time and I will log off when I leave for the day.

- To prevent others from obtaining my password via "shoulder surfing", I will shield my keyboard from view as I enter my password.

- I will not engage in, encourage, or conceal any hacking or cracking, denial of service, unauthorized tampering, or unauthorized attempted use of (or deliberate disruption of) any data or component within the interoperable system(s) and IPAWS-OPEN.

- I agree to inform my Local System Administrator when access to the interoperable system(s) and/or IPAWS-OPEN is no longer required.

- I agree that I have completed Computer Security Awareness training prior to my initial access to the interoperable system(s) and IPAWS-OPEN and that as long as I have continued access, I will complete

Computer Security Awareness training on an annual basis.

**2.6 Accountability**

- I understand that I have no expectation of privacy while using any services or programs interoperating with IPAWS-OPEN.
- I understand that I will be held accountable for my actions while accessing and using interoperable system(s) and IPAWS-OPEN, including any other connected systems and IT resources.
- I understand it is my responsibility to protect sensitive information from disclosure to unauthorized persons or groups.
- I understand that I must comply with all software copyrights and licenses pertaining to the use of IPAWS-OPEN.

**2.7 Incident Reporting**

- I will promptly report IT security incidents, or any incidents of suspected fraud, waste or misuse of systems to the Local System Administrator and/or the Gallatin County Emergency Management Help Desk.

**3.0 IPAWS-OPEN Rules of Behavior Statement of Acknowledgement**

*I have read and agree to comply with the requirements of these Rules of Behavior. I understand that the terms of this agreement are a condition of my initial and continued access to* Gallatin County Emergency Management Interoperable System(s) *and IPAWS-OPEN and related services and that if I fail to abide by the terms of these Rules of Behavior, my access to any and all IPAWS-OPEN information systems may be terminated and I may be subject to criminal or civil prosecution. I have read and presently understand the above conditions and restrictions concerning my access.*

Name (Print): _____

Signature: _____ Date: 6-2-16