FAQ: Cybersecurity and ShakeAlert® System Resilience

The ShakeAlert® Earthquake Early Warning (EEW) system must comply with the federal government’s cybersecurity Assessment and Accreditation (A&A) process, as required by the Federal Information Security Management Act (FISMA) of 2002. The U.S. Geological Survey (USGS) ShakeAlert completed this process and received a conditional Authority to Operate (ATO) in March 2018. The US Department of Homeland Security (DHS) considers the ShakeAlert System a “Highly Valued Asset” that meets internal government requirements and standards, as well as industry standards for network security architecture.

How is the ShakeAlert System designed?

The ShakeAlert System architecture (shown here) connects seismic data from the field to subscribers of ShakeAlert Messages. Data processing begins with the Data Layer, which streams seismic data from the field into four operations centers (Pasadena, CA; Menlo Park (Mountain View), CA; Berkeley, CA; and Seattle, WA).

If seismic activity is detected, amplitude and time parameters flow upward to the Production Layer and are evaluated for earthquake characteristics. If an earthquake is detected, the system estimates its location, magnitude, and shaking intensity.

Real-time ground motion data from ShakeAlert sensors is processed at four sites: Seattle, Pasadena, Menlo Park, and Berkeley. Earthquake detection algorithms at each site communicate with one another to determine the earthquake magnitude and intensity. Earthquakes larger than a minimum threshold are redundantly sent to the alert modules in Seattle, Pasadena, and Menlo Park. Technical Partners can subscribe to read-only alert modules at each location. Each arrow on the chart represents data transfer mediated by ActiveMQ message brokers.

Subscribers/Technical Partners

Alert Layer

Alert decision module
Seattle

Alert decision module
Pasadena

Alert decision module
Menlo Park

Security Barrier

Production Layer

Earthquake detection

Waveform Processors

Seattle

Pasadena

Menlo Park

Berkeley

Data Layer

1 When referring to "system" vs "System," lowercase "s" refers to the USGS part of the operation (sensors and processing centers), and uppercase "S" refers to the USGS part and the alert delivery Technical Partners (i.e., the entire System).
Earthquakes estimated to meet a USGS-defined magnitude and shaking intensity threshold are released to the Alert Layer as ShakeAlert Messages. Subscribers access Messages on ActiveMQ message brokers by monitoring one or more of the USGS Alert Layer servers. A USGS License Agreement is required to subscribe to ShakeAlert Messages.

How is the ShakeAlert System protected against hacking?
ShakeAlert administrators use a variety of protective tactics to guard against malicious activity. Only administrators can access the USGS Alert Layer servers and must use two-factor authentication via a hardware token. Technical Partners have read-only access to ShakeAlert Message brokers.

Regular security tests are performed, including weekly vulnerability scans, monthly security patching, and annual penetration testing by an outside firm. All changes to servers are performed by configuration management software; if any data or software on the servers change, administrators are notified by email and SMS. All servers are monitored with Nagios XI that detects any uncommon activity.

Are ShakeAlert System servers located on premise or in the cloud?
Redundant ShakeAlert Alerting Centers are located on premise in secure locations in Pasadena, Menlo Park (Mountain View), and Seattle.

Who is authorized to access the ShakeAlert System?
Public and private partners who have valid USGS License Agreements, referred to as ShakeAlert Technical Partners, may access ShakeAlert Alert Layer servers and have read-only connections to Alert Layer message brokers. Neither Technical Partners nor any member of the public can login or post messages to Alert Layer servers. Technical Partners connect to message brokers by username/password. A random eight-character password is generated for Technical Partners.

ShakeAlert administrators are USGS employees or USGS-credentialed civilians who are vetted IT professionals. Remote access by administrators to the ShakeAlert system requires a secure shell with two-factor authentication, which is performed via a hardware token. Firewall rules block contact from the public internet. No external logins or database access are allowed.

How is this access monitored?
USGS monitors and logs connections and locks accounts with any suspicious activity. The US government will share any security breach-related information on a need-to-know basis per the terms of ShakeAlert License Agreements.

Who performs development work in the ShakeAlert System?
Development work on ShakeAlert is conducted by USGS employees or those associated with the USGS though a formal agreement (e.g., university personnel or contractors). Development follows a disciplined process of testing and staging. Approved software is deployed to production only by USGS employees and/or USGS-credentialed civilians.

Are connections to the ShakeAlert System encrypted?
Yes. All subscriptions to ShakeAlert are performed over a Transport Layer Security (TLS) connection. TLS is a cryptographic protocol that provides end-to-end security of data sent over the internet. Data transfers between servers within the ShakeAlert System are also done over TLS.
Is any part of the System internet-facing?

Yes, the message broker ports on the Alert Layer servers are public-facing, allowing read-only access to XML messages. The servers are hardwired for internet connectivity; no wireless access is allowed. Alert Layer message brokers do not accept incoming messages from public connections. No email or web browsing is possible on the servers. Data Layer servers are not internet-facing and get their earthquake data stream through a private network.

Additional information on ports and protocols is made available to Technical Partners with Pilot or License to Operate (LtO) Agreements.

How does ShakeAlert comply with accepted network security architecture standards?

The ShakeAlert System uses multiple tiers of servers. Publicly accessible servers are separated from the computing and processing servers. Redundancy is built into the ShakeAlert architecture. No data is kept on ShakeAlert servers for any length of time. Servers can be rebuilt using a combination of kick-start and configuration management in approximately one (1) hour.

What plans are in place for interruptions or failures?

The ShakeAlert System has a Business Impact Assessment (BIA) and a Disaster Recovery Plan (DRP) in place. The BIA is used to determine criticality of an interruption and to develop incident-specific disaster recovery strategies. These plans meet the US Department of Homeland Security High-Value Asset requirements and are regularly tested.

What cybersecurity threats should be considered and monitored?

XML injection attacks can be a serious threat vector. Only USGS employees have access to the Production and Alert Layer servers. Remote access to production ActiveMQ message brokers is limited to a narrow whitelist of other Production Layer ShakeAlert instances. There is no communication between Alert Layer servers.

Threats to Production Layer servers are managed by blocking public visibility of the servers. Shell access is limited to ShakeAlert administrators connecting with two-factor authorization from secured hosts at ShakeAlert operations centers.

---

Accessing ShakeAlert Technical Resources

For access to more information about system ports, protocols, etc., Technical Partners may contact:

USGS Technical Engagement Coordinator Robert de Groot
rdegroot@usgs.gov