IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

CISA Central Reporting

DEFEND TODAY, SECURE TOMORROW

OVERVIEW

The Cybersecurity and Infrastructure Security Agency's (CISA) 24x7x365 operations center is called CISA Central. CISA Central provides situational awareness and near-real time operational reporting on events impacting the nation's 16 critical infrastructure sectors. Our guiding principles in publishing notifications are to avoid strategic or operational surprise and to inform ongoing or near-term operations and decisions.

CISA CENTRAL REPORTING ACTIVITY

CISA Central produces two daily reports and four types of notifications, as described in the table below:

Product Name	Purpose/Description	Target Audience
Operations Summary (OPSUM)	• A daily report that provides situational awareness on significant current operations. TLP:RED.	CISA Leadership, select CISA staff and partners
Daily Operations Report (DOR)	• A daily report that provides updates on ongoing CISA operations. TLP:AMBER.	Federal, State, Local, Tribal, Territorial (FSLTT) government and Industry partners
Senior Leadership Note (SLN)	• An event-driven report that alerts Senior Leadership of an emerging incident or event. • May be triggered by a PCIR or CIR event. • May contain restricted information, such as victim identity or law enforcement sensitive data.	Limited, DHS-only audience
Awareness Message (AM)	• An event-driven report that signals that CISA is interested in the event. • May meet a PCIR or CIR and require an SRMA notification. • Impacts one or more critical infrastructure sectors. • Will not include restricted information.	CISA plus inter- and intra-governmental partners (FSLTT)
Situation Report (SITREP)	• An event-driven report that details an ongoing physical, communications, or cyber event/incident, such as a hurricane or wildfire, that has an impact to one or more critical infrastructure sectors. • Firsthand information is from a trusted source. • Initial reports are sent within 60 minutes and are typically followed by scheduled updates.	Broad distribution to CISA partners
Ransomware Reporting Summary	• A daily report that lists ransomware events that Central was informed about in the last 24 hours. TLP:GREEN. • No victim identification in the report. • Central follows up with a more detailed, TLP:RED version of this report sent to each affected region and SRMA, as appropriate.	CISA Leadership, CISA Regions and select CISA staff

For more information or to seek additional help, contact us at central@cisa.dhs.gov.