TLP:CLEAR

Communicating Under Pressure: Best Practices for Service Providers

Publication: September 2, 2026

U.S. Cybersecurity and Infrastructure Security Agency
U.S. Federal Bureau of Investigation
Australian Cyber Security Centre
Canadian Centre for Cyber Security
New Zealand National Cyber Security Centre
U.K. National Cyber Security Centre

TLP:CLEAR

Guidance at a Glance

Title	Communicating Under Pressure: Best Practices for Service Providers
Original Publication	**September 2, 2026**
Executive Summary	Service outages impacting IT and operational technology (OT) systems can be damaging and disruptive for customers, network defenders, critical infrastructure owners and operators, and the general public. During incidents that reach or exceed established thresholds, whether caused by malicious activity or a non-malicious event, service providers must communicate effectively so end users can minimize operational impact. This guide outlines how to prepare for effective outage communications and key elements of clear, actionable messaging. Effective communication begins with a factual summary tailored to predefined audiences, avoids PR spin, and adheres to regulatory requirements. Service providers should be transparent by sharing what is known, unknown, and under investigation, while providing frequent, iterative updates as new information emerges or circumstances change.
Key Actions	▪ Develop a communications plan with defined incident thresholds and target audiences for communications. ▪ Practice transparency and avoid PR/marketing language. ▪ Provide technical information and a root cause analysis for end users. ▪ Align all messaging with legal and regulatory requirements.
Intended Audience	**Organizations:** Government; Federal Civilian Executive Branch (FCEB); State, Local, Tribal, and Territorial (SLTT); Critical Infrastructure. **Sectors:** Critical Manufacturing, Information Technology, Energy, Water and Wastewater, Transportation, Communications. **Roles:** Defensive Cybersecurity Analysts, Executive Cybersecurity Leadership, Cybersecurity Legal Advisors, Technical Support Staff, Incident Responders, Public Relations Specialists.

This publication was prepared by the CISA with contributions from the FBI, NCSC-UK, Cyber Centre, NCSC-NZ, and ASD's ACSC. It reflects best practice within the United States, not Australia. This document was not prepared in consideration of Australian law and does not reflect the reporting obligations placed on Australian companies.

For more information on Australian cyber incident reporting requirements, consider guidance on Australian incident reporting obligations. For example:

- *Report | Cyber.gov.au*
- *SOCI Act regulatory obligations*
- *https://www.cisc.gov.au/resources-subsite/Documents/overview-cyber-security-obligations-corporate-leaders.pdf*

Information provided to the Australian Signal Directorate's Australian Cyber Security Centre regarding a cyber incident may be protected by the Limited Use regime, which protects how the information is used within the Australian Government.

Introduction

Effective communication during IT and operational technology (OT) service outages is as critical as technical remediation in limiting harm and operational impact. A disruption at one organization (whether from natural hazards, human error, equipment failure, or malicious activity) can cascade across interconnected systems. Speculation and uncertainty from end users regarding the nature of the disruption can make things worse.

Informed by real-world events such as the Nov. 18, 2025, Cloudflare outage[1], this guidance emphasizes clarity, accountability, and transparency as core principles. It outlines how organizations can prepare the delivery of timely, accurate information in advance and provides best practices for communicating with stakeholders during major service disruptions, including elements of effective messaging.

Why It Matters

Service outages alone have the potential to cause enough damage, disruption, and societal panic without speculation and uncertainty from end users and the public as added factors. Moreover, with the evolving and heightened geopolitical tensions around the world, it is important to identify the confirmed, **known** cause upfront and clearly articulate what it is and what it is not to predefined audiences. If the root cause is still under investigation, it is equally important not to release premature conclusions. Effective communication gives important context for readers, limits speculation, and drives the focus toward the root cause, mitigations, and solutions. However, when service disruptions are known to be—or even suspected to be—caused by cyber threat actors, it is critical that any outward communications account for operational security and align with any law enforcement investigations or containment efforts.[2]

Preparing Your Organization to Communicate Effectively

The authoring agencies recommend service providers develop a service outage communications plan that defines triggers, escalation paths, and procedures and includes templates for status pages; customer and partner notices; and regulatory communications. To communicate effectively during an outage, service providers should establish and exercise the following key structures before a crisis:

- **Cross-functional incident team.** Include engineering and operations, communications and public affairs, legal, risk and compliance, and customer support and sales, with primary and alternate points of contact.
- **Government relations.** Consider including a government relations lead in cases where government stakeholders are affected by incidents.

---

[1] The Cloudflare Blog, "Cloudflare outage on November 18, 2025," accessed April 30, 2026, https://blog.cloudflare.com/18-november-2025-outage/.

[2] Communications should balance transparency with the need to avoid compromising the investigation, exposing organizations to heightened risk, encouraging further attacks, or causing a cyber threat actor to change tactics before response activities are complete.

  - **Government relations lead.** This point of contact helps ensure messaging to government agencies and other officials remains consistent with public communications.
- **Clear roles and authority.** Designate an incident lead, communications lead, and a spokesperson with predefined approval paths and escalation criteria.
  - **Incident lead.** This point of contact orchestrates the organization's response to the cyber incident.
  - **Communications lead.** This point of contact functions as the orchestrator and manages the information that is coordinated internally and externally.
  - **Spokesperson.** This point of contact functions as the sole public-facing representative who delivers approved statements or responds to questions from reporters.
- **Parallel, synchronized workstreams.** Technical teams diagnose and remediate the root cause, communications manage public messaging and stakeholders, and leadership drives strategy and regulatory outreach.
  - Use designated liaisons, scheduled syncs, and a single intake path to align facts and shield engineers from external interruptions.
- **Legal team.** The legal teams help ensure communications, regulatory obligations, contractual considerations, and risk management activities are appropriately aligned throughout the incident.
- **Backup communications methods.** Establish and regularly test backup communication methods for informing internal and external stakeholders (e.g., backup email and messaging, SMS and phone trees, radios, out-of-band communications, and conference bridges) for moments where primary systems are degraded or compromised.
- **Pre-planned playbooks and procedures.** Communication plans should have defined triggers, escalation paths, and procedures and should be reviewed and refreshed regularly.
  - Execute plans regularly with periodic training, such as simulated tabletop exercises, to help ensure communications teams can respond effectively under pressure.
- **Message consistency.** Ensure messaging to internal audiences is consistent with external communications, when possible.
  - Consider providing all staff with approved talking points or instructions to direct questions to designated communications channels.

Key Elements of Effective Messaging

Effective outage communication requires clear, timely, and audience-appropriate messaging that supports rapid decision-making during high-pressure events. The following elements outline how service providers can maintain trust, deliver actionable information, and uphold transparency throughout an incident response cycle.

Understanding The Issue

During widespread outages, organizations need immediate, accurate, and concise information to limit harm and preserve trust. Service providers should communicate confirmed facts early and clearly state

what the issue is, and what it is not, for predefined audiences. If the root cause is under investigation, avoid premature conclusions. Furthermore, if the service provider suspects or can confirm malicious cyber activity, ensure external communications protect operational security and align with law enforcement investigations or containment efforts.

Know Your Audience

The authoring agencies recommend service providers segment communications so each audience (technical, executive, public) can effectively act on relevant information and keep updated contact lists to help enable staff to engage the appropriate offices in the event of a crisis. Audiences may include:

- Enterprise IT teams and security operations centers.
- An affected organization's employees, and customers.
- Government partners, leaders, and regulators.
- Critical infrastructure owners and operators.
- Media and the general public.

Critical infrastructure owners and operators are actively implementing mitigations and making risk-based decisions in real time based on service providers' guidance. Best practices include:

- **Prioritize technical specificity** and operational relevance.
- **Provide operational impact statements**, not just symptoms.

Lead with a Concise Summary

In the event of an outage, customers, network defenders, and critical infrastructure owners and operators need to receive vital information as efficiently and concisely as possible, to aid in rapid response and recovery.

Best practices include:

- **Lead with an overall "bottom line upfront"** that is useful for both the general public and a technical audience.
  - Include affected systems, what users experienced, scope, and known cause without speculation.[3]
- **Avoid vague language** (e.g., "service degradation").
- **Design messaging for rapid comprehension** under pressure, using concise headings and prioritized information.

[3] Use a risk-informed approach when deciding what technical details or specific system information to include because some details may enable cyber threat actors to target other customers with similar system configurations.

Practice Transparency and Accountability

Service providers can help instill trust with their customers by being upfront about an outage or incident, even when information is unknown or unconfirmed.

Best practices include:

- **State what you know and what you do not know.** Honest, transparent admissions of uncertainty are more effective than silence and speculation.
  - Transparency must align with the nature of the incident.
    - For **active cyber incidents**, sharing too many details could jeopardize detection, investigation, and containment.
    - For **non-malicious outages**, forthcoming transparency should be the default.
- **Use a single source of truth**, such as a status webpage or blog post, for public updates.
- **Focus on actionable information, not reputation management.**
  - Provide clear guidance that outlines specific actions that customers should take, or;
  - Clearly convey if no action is necessary for customers.
- **Avoid front-loading communications with reassurances, generalities, or marketing language**.
- **Acknowledge the impact** and commit to fixes and restoration.

Provide Continuous, Time-Stamped Updates

Regular updates are critical during an event to limit speculation and indicate to your audiences that you are actively working and addressing the issue.

Best practices include:

- **Share a clear timeline** of the incident or outage.
- Include timeline of actions taken and recovery milestones.
- Timestamp updates, **even when there is no new information.**
- Maintain a single source status page.

Maintain Compliance with Regulatory and Reporting Requirements

Certain legal considerations may need to be taken into account when externally communicating about an outage or incident.

Outage communications may trigger legal obligations, including:

- Incident reporting disclosure rules.
- Sector-specific mandates (e.g., Financial Services, Healthcare, Transportation, etc.).
- Contractual service level agreements (SLAs).

Best practices include:

- **Align messaging** with legal counsel and compliance teams.
- **Ensure consistency** across public statements and regulatory findings.
- **Coordinate appropriately with government or law enforcement partners** before making public attribution statements.

Incorporate Expected Product Security Improvements

Post-incident communications should discuss how service providers intend to use lessons learned to enhance products and processes. Considerations include:

- Incorporating Secure by Design Principles and a commitment to products configured with enhanced safety features by default.
- Transparently discussing vulnerability management and patching.

Key Takeaways

Effective outage communications should be:

- **Immediate**. Acknowledge quickly.
- **Technical**. Provide actionable guidance.
- **Transparent**. Share what you know (and do not know).
- **Accountable**. Own your responsibilities and the outcomes.
- **Iterative**. Update continuously.

Resources

For more information on incident response and communication, see:

- The NIST Cybersecurity Framework (CSF) 2.0 – 5. Improving Cybersecurity Risk Communication and Integration
- NIST SP 800-150: Guide to Cyber Threat Information Sharing
- NIST SP 800-61: Incident Response Recommendations and Considerations for Cybersecurity Risk Management
- Guidance on Effective Communications in a Cyber Incident

Disclaimer

The information in this report is being provided "as is" for informational purposes only. CISA and the authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities,

products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA and the authoring agencies.

Acknowledgements

This publication was informed by trusted industry partners, including Microsoft, Sophos, Cloudflare, and American Water.

Version History

Sep. 2, 2026: Initial version.

References

The Cloudflare Blog. "Cloudflare outage on November 18, 2025." Accessed April 30, 2026. https://blog.cloudflare.com/18-november-2025-outage/.