800-61 and potential updates for AI cybersecurity incidents

Alex J. Nelson, Ph.D.
Computer Scientist
NIST / ITL / CSD

2026-05-14

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Incident Response document history

1991:
800-3

2004:
800-61

2012:
800-61r2

2014:
CSF

2025:
800-61r3

800-61: assists with building a new function within organizations.

800-61r3: builds on CSF having incident response as integral to cybersecurity strategy.
Document is “CSF Community Profile,” for community: *all incident response teams*.

Potential 800-61 updates for AI

- "Community" is every org's incident response teams; guidance is for cybersecurity incidents.
- Incidents can happen with AI in various event-specific roles
  - *Victim* or *target* (fulfilling working definition shared with CISA playbook)
  - *Deceiver*, serving attacker (stronger phisher) or defender (honeypot) (*outside* working definition shared with CISA playbook)
  - *Force-multiplier*, serving attacker (autonomous campaign executor) or defender (intrusion detection)
- What example incidents motivate new 800-61 guidance?
- Some incidents could have AI only used on attacker side. What is the guidance appropriate for current community of 800-61?
  - 800-61r3 does not presume adoption of AI on defender side.
  - Mind: **Community** of AI CSF Profile (NIST IR 8596) and its "Thwart" focus.