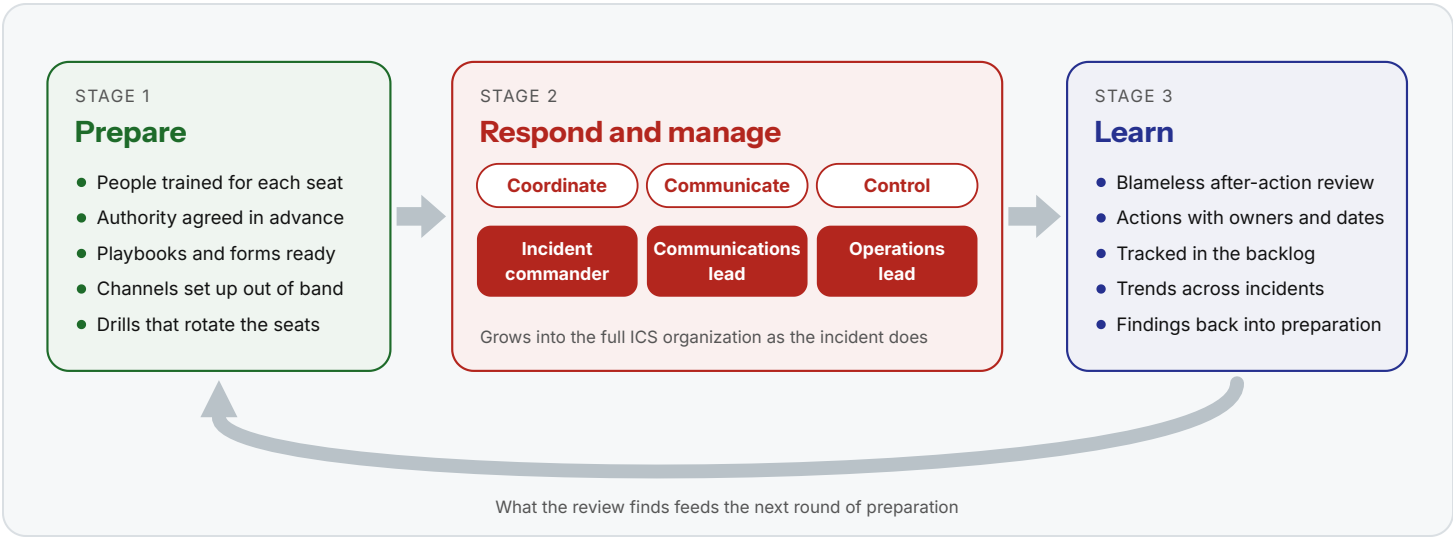
Incident Command

A NIMS-based guide to running incidents. Written for cybersecurity. Works for anything.

Written by Habib Tora · v1.0 · September 2026

Any organization large enough to have incidents will eventually have one that outgrows the team that found it. How that incident goes depends on three things: whether someone is clearly in charge, whether everyone hears the same facts, and whether the work is planned or improvised. The National Incident Management System answers all three, and emergency services in the United States have run on it for two decades.

This guide adapts NIMS to cybersecurity. The structure, vocabulary and paperwork carry over almost unchanged. What changes is who fills each seat and what each section does. It is laid out the way Google's SRE team presents its own ICS-based process, in three stages: prepare, respond and manage, learn. Nothing here depends on the incident being cyber.



Coordinate
One commander, one set of objectives, one plan per operational period

Communicate
Every audience hears the same facts, on a schedule, from one voice

Control
Clear assignments, a manageable span of control, nobody freelancing

Prepare

Most of what decides an incident is settled before it starts. The people for each seat are trained and have practised in it. The authority to isolate systems, suspend accounts and spend money is agreed. The channels, forms, contracts and playbooks are ready to use at two in the morning. Prepare lists what to have in place.

Respond and manage

The first qualified person takes command out loud. Three roles cover most incidents: an incident commander who coordinates, a communications lead who keeps every audience informed, and an operations lead who runs the technical work. When the incident outgrows one shift or one team, the rest of the ICS organization fills in around them: planning, logistics, finance, liaison, safety.

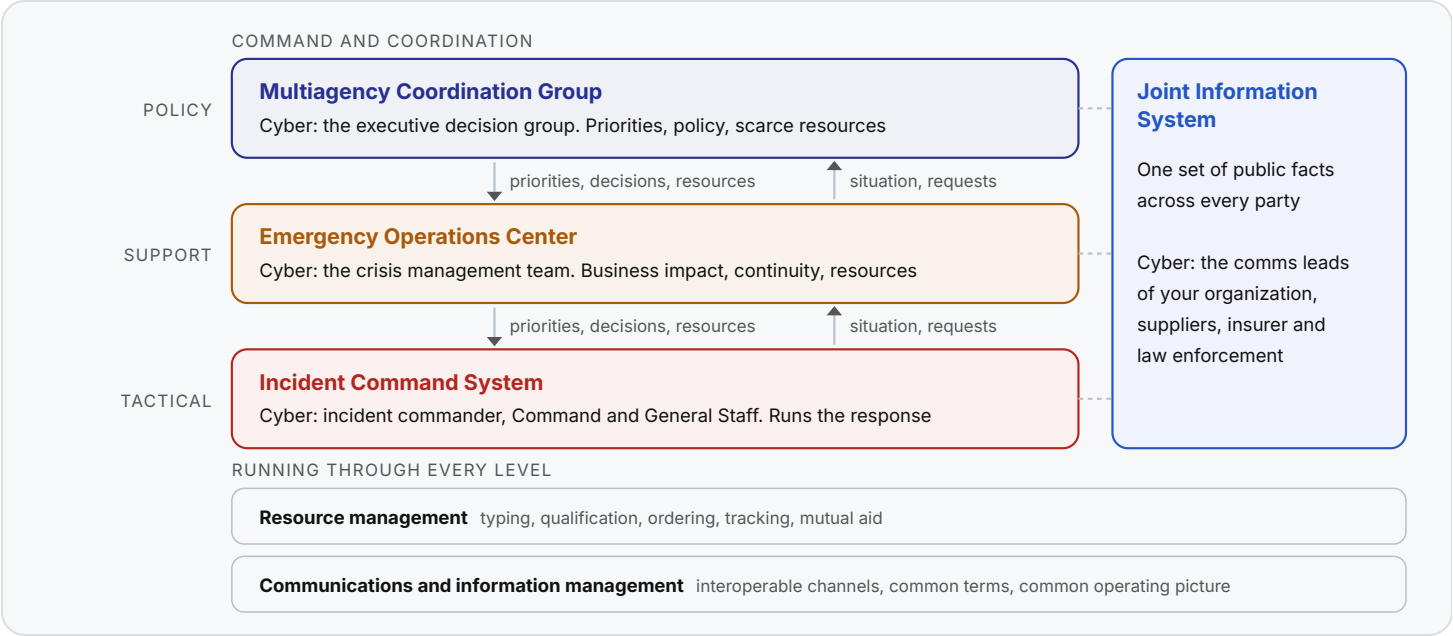
Each operational period gets written objectives and an Incident Action Plan. Command changes hands by briefing. Nobody joins the response without an assignment. Respond and manage covers the organization, sizing, the planning cycle, unified command, communications and handover.

Learn

The after-action review starts as soon as the incident closes, while memory is fresh. It is blameless: people acted on what they knew at the time, so findings go to systems, procedures and training. Every corrective action gets an owner and a date and is tracked to done. Across many incidents, recurring findings show where larger investment belongs. Learn has the review questions and the improvement plan.

NIMS in one picture

ICS is one part of NIMS. The rest adds a crisis team and an executive group above the incident, one joint voice to the public, and common ways to handle resources and information at every level.



NIMS at a glance walks through the three components and the four structures.

How it pairs with PIVTR-D

PIVTR-D covers the response lifecycle, the technical work from preparation to debrief. This guide covers the management around that work: who decides, how the team is organized, how the plan is written and handed over, and how the effort holds up past the first night.

PIVTR-D phase	Where it sits in incident command
Preparation	Prepare: people qualified for each seat, pre-agreed authority, the forms, the communications plan
Identification	Outside the incident organization until an event of interest is raised

PIVTR-D phase	Where it sits in incident command
Verification and triage	Initial response and assessment. The first qualified responder takes command and sizes the incident
Response loop	The Operations Section, working to one set of objectives per operational period, carried in the Incident Action Plan
Debrief	Demobilization, then Learn

When to stand it up

Use the structure when an incident needs more than one team, will run past one shift, or will draw in executives, counsel or outside parties. An analyst closing a phishing report needs none of it beyond knowing they are in command. An enterprise ransomware event needs most of it by the end of the first day. Sizing the response sets the thresholds.

Further reading

- National Incident Management System, Third Edition, FEMA, 2017
- Incident Management Guide, Google SRE
- Managing Incidents, ***Site Reliability Engineering***, chapter 14
- Incident Response, ***The Site Reliability Workbook***, chapter 9
- Postmortem Culture, ***Site Reliability Engineering***, chapter 15
- PIVTR-D, the companion incident response field manual

Quick card

The first thirty minutes of command, and what to fill as it grows.

First thirty minutes

#	Item
1	Take command out loud: your name, the time, the incident name, the channel. Open your activity log.
2	Size up: what happened, what is affected, what is still happening, what is unknown.
3	Set up to three objectives, each with a measure and a time.
4	Name an Operations lead and hand the technical work to them. Stay off the keyboard.
5	Open a command bridge and an out-of-band channel. Treat email, chat and identity as visible to the attacker until scoping shows otherwise.
6	Decide the incident type, 5 to 1, and fill the positions it calls for.
7	Tell counsel if personal data, regulators, law enforcement, extortion or insurance may be involved.
8	Set the time of the first briefing and the first executive update.
9	Write the incident briefing (ICS 201) before the first briefing.
10	Check hours: who has been awake since when, and who relieves them.

Positions by incident type

Type	Fill
5	Incident commander, often the analyst who found it
4	The core three: IC, Communications lead, Operations lead
3	IC, Operations, Planning, Communications, Liaison, with Legal advising. Safety once shifts run long

Type	Fill
2	All Command and General Staff. Unified command if another party holds authority. Crisis team (EOC) active
1	All positions, deputies for key roles, unified command with outside authorities. Crisis team, executive group and joint information system active

Each operational period

1. Objectives meeting
2. Tactics meeting
3. Planning meeting
4. IAP approved by the IC
5. Operations briefing, and the period starts
6. Execute and assess, with status to Planning
7. Executive updates at the times the IAP sets

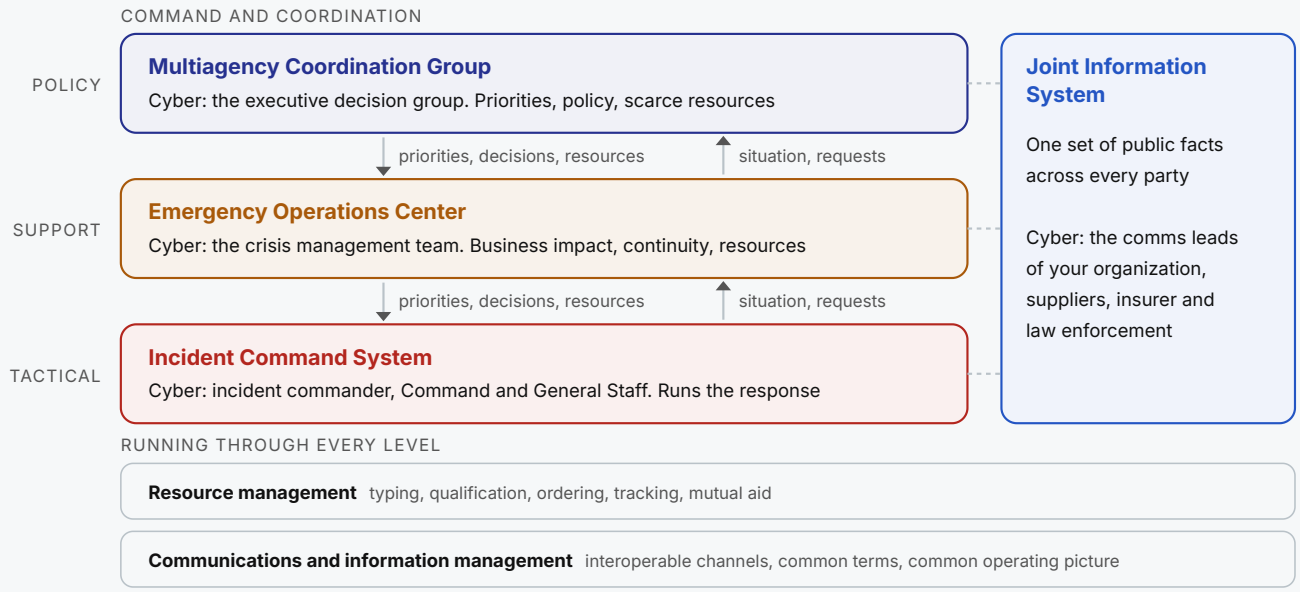
Rules at every size

- One incident commander, named out loud.
- One boss per responder for the length of the incident.
- Three to seven people per supervisor. Split the work at seven.
- Written objectives before tactics.
- One voice to executives and the public, through the Public Information Officer.
- Every update answers: what is affected, how bad, what to do now, and when it will be fixed or the next update is due.
- Handover by briefing, announced to everyone, logged with the time.
- Nobody joins the response without an assignment.

NIMS at a glance

The National Incident Management System is FEMA's framework for how organizations work together on incidents of any kind and size. It was first issued in 2004. The current version is the Third Edition, published in October 2017.

The Incident Command System is its best-known part. NIMS also covers how resources are described, ordered and tracked, how information is shared, and three structures that sit above the incident for support, policy and public information.



NIMS command and coordination, from the incident up to policy, with the two components that run through every level.

Three components

Component	What NIMS covers	In a cyber incident	In this guide
Resource management	Typing, qualifying, ordering, tracking and releasing people, teams, equipment and facilities, plus mutual aid	Who can fill each seat, what the retainer firm provides, how extra analysts and rebuild hardware are requested and tracked	Resources

Component	What NIMS covers	In a cyber incident	In this guide
Command and coordination	ICS at the incident, emergency operations centers, multiagency coordination groups, and the joint information system	Incident command for the response, a crisis team for business impact, executives for policy, one voice to the public	The organization, Above the incident
Communications and information management	Interoperable communications, common terminology, and a common operating picture	Out-of-band channels, one glossary, one status summary and timeline everyone works from	Communications and information

Four command and coordination structures

Structure	Level	Does	Cyber equivalent
Incident Command System	Tactical, at the incident	Directs the response	Incident commander, Command and General Staff
Emergency Operations Center	Support	Supports incident command with resources, information and decisions, and manages consequences away from the incident	Crisis management team, business continuity
Multiagency Coordination Group	Policy	Sets priorities and allocates scarce resources across incidents and organizations	Executive decision group
Joint Information System	Across all levels	Coordinates public information across every organization involved	Communications leads of every party, working from one set of facts

Management characteristics

NIMS names fourteen management characteristics that hold every structure together, from common terminology to accountability. Principles lists all fourteen with their cyber meaning.

Training

FEMA's Emergency Management Institute teaches NIMS in free online courses. IS-700 introduces NIMS, IS-100 and IS-200 cover ICS, and IS-703 covers resource management. ICS-300 and ICS-400 are classroom courses for people who will command larger incidents.

Prepare

Incident command is mostly people and paperwork, and both have to exist before the incident does. The technical preparation lives in the PIVTR-D preparation playbook. This page covers what the incident organization needs in place before anyone stands it up.

People

Name at least two trained people for every seat you expect to fill, so the incident survives its first shift change. Training covers the role, the forms and the meetings. Weight it toward the incident commander, the one job nobody does day to day.

Practise in the seats. Google runs Wheel of Misfortune exercises, role-playing past incidents so less experienced on-callers build skill somewhere safe. Run tabletops the same way: replay real incidents, rotate who holds command, communications and operations, and time the first objectives and the first executive update.

Authority

Write down what the incident commander can do without asking: isolate systems, suspend accounts, take services offline, activate retainers, spend up to a set amount, engage law enforcement. Put the limits in business terms. Name who approves anything above them, and their backups.

Detection that reaches someone

The incident organization starts when someone is paged. Google's guide asks four things of an alert: it arrives in time, it covers what users depend on, it measures what users experience, and someone can act on it. For security, read that as detections that fire early enough to contain, cover the systems and identities that matter most, carry enough context to size the incident, and route to someone who can take command. The PIVTR-D identification playbook covers the detection side.

Tools that open the incident for you

Automate the first ten minutes so responders spend them thinking. One action should open the incident record from the ICS 201 template, create the command bridge and the out-of-band room, page the incident commander and on-call, start a timestamped activity log, and post the first internal notice. Google's guide points the same way: automate common tasks and the first read of impact so on-callers can work the problem.

Contracts and outside help

- Incident response retainer: how to activate it, response times, who can sign.
- Cyber insurance: notice deadline, panel vendors, what the insurer must approve.
- Counsel: who to call, and when counsel directs the investigation.
- Managed providers: which containment actions they take on their own authority.

- Law enforcement: named contacts, agreed before you need them.

Ready to run an incident

#	Item
1	Two trained people named for incident commander, operations, communications and planning
2	Incident commander authority written, with limits and approvers
3	Incident types mapped to your severity scale and published
4	Forms and the incident record template ready to copy
5	Out-of-band channel and accounts provisioned outside the main identity provider
6	Contact roster for internal and outside parties, kept offline and tested
7	Retainer, insurer and counsel details in the roster
8	One action that opens a new incident
9	Shift length and relief rules agreed
10	A tabletop in the last quarter, with the seats rotated

Respond and manage

Google's incident guide says it plainly: left unmanaged, a response turns chaotic. Treat it as a project in its own right, with someone planning it, someone deciding who is involved, and a record of what was done. ICS is the structure for that project.

ICS came out of the California wildfires of the 1970s, when agencies fighting the same fire used different terms, different radios and different plans. Cyber incidents break down in the same places: nobody sure who decides, three people briefing executives with three different numbers, responders on hour thirty with no relief, and a vendor, counsel and an insurer each running their own version of the response.

Coordinate, communicate, control

Google's incident management system, IMAG, is built on ICS and organizes around three Cs. Each maps onto NIMS positions.

C	What it means	Held by
Coordinate	One set of objectives and one plan, with every responder working to it	Incident Commander, Planning
Communicate	Every audience hears the same facts on a schedule, and incoming requests have one door	Public Information Officer, Liaison
Control	Clear assignments, a manageable span of control, and changes made through command	Incident Commander, Operations

Start with three roles

Most incidents need three seats filled. Google's guide names the same three.

Role	NIMS position	Google IMAG	Owns
Incident commander	Incident Commander	Incident Commander (IC)	The overall response: objectives, priorities, decisions, handover
Communications lead	Public Information Officer	Communications Lead (CL)	Regular updates to every audience, and the single contact for incoming questions

Role	NIMS position	Google IMAG	Owns
Operations lead	Operations Section Chief	Operations Lead (OL)	Mitigating the issue, limiting impact, resolving the problem

Incident roles go to whoever knows the systems and the situation best. Day-job reporting lines pause until the incident closes.

The full organization

When the incident runs past one shift or one team, the rest of the structure fills in around those three.

Command
Sets objectives, approves the plan, speaks for the incident

Operations
Does the response work

Planning
Knows the situation, writes the plan, keeps the record

Logistics
Gets responders what they need

Finance/Admin
Tracks time, cost, contracts and claims

Getting more help

NIMS describes Incident Management Teams: rostered groups of ICS-qualified people, typed by capability, who deploy to manage incidents that outgrow local capacity. Google keeps the same capability as Incident Response Teams it can activate for major incidents. In cyber, the equivalents are an internal major-incident team drawn from across the organization, the incident response firm on retainer, and an executive crisis team for decisions above the incident commander's authority. Decide in advance who activates each one, and how.

In this section

Page	Covers
Principles	The fourteen NIMS management characteristics, in cyber terms
The organization	Every seat, what it owns, who fills it
Sizing the response	Complexity types, and when to grow or shrink
The planning cycle	Operational periods, the meetings, the Incident Action Plan
Unified command	Several parties with authority running one response
Above the incident	The crisis team, the executive group and the joint information system
Resources	Typing, qualification, the six-step resource process, mutual aid

Page	Covers
Communications and information	Channels, cadence, what every update answers, the common operating picture
Command and handover	Taking command, transferring it, shift change
Demobilization	Releasing people and closing the incident organization

Principles

NIMS names fourteen management characteristics. Together they let people who do not normally work together run one response. The right-hand column is what each looks like in a cyber incident.

Characteristic	In NIMS	In a cyber incident
Common terminology	Plain language and defined terms across every organization involved	One name per system, one severity scale, one agreed meaning for contained. Publish the glossary before the incident.
Modular organization	The organization grows from the top down only as far as the incident needs	Start with an incident commander. Add sections when workload or span of control calls for them, and fold them back when it drops.
Management by objectives	Command sets objectives, the sections choose tactics to meet them	An objective names an outcome, a measure and a time, such as no attacker access to domain controllers by 18:00. Tasks sit below it in assignments.
Incident action planning	A plan for each operational period, written once the incident is large enough	The IAP says what this period is for, who does what, how people talk to each other, and when the next briefing is.
Manageable span of control	NIMS treats one supervisor to five people as optimal. ICS training uses three to seven as the working range	When a lead has more than seven people reporting, split the work into groups with their own supervisors.
Incident facilities and locations	Command post, staging areas, bases	The war room, physical or virtual, a clean build network, the evidence store, somewhere to sleep.
Comprehensive resource management	Identify, order, track and release resources	Retainers, forensic licences, loaner hardware and extra staff are ordered through Logistics and tracked until returned.

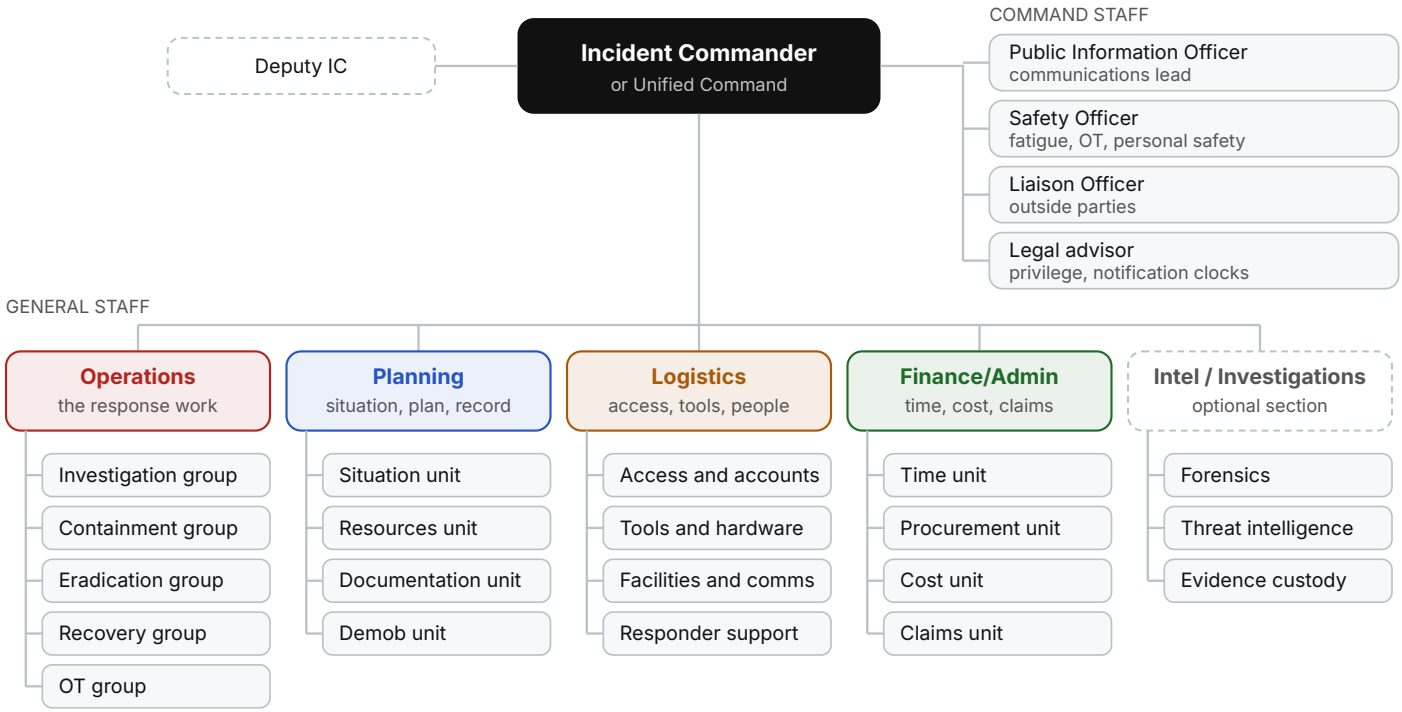
Characteristic	In NIMS	In a cyber incident
Integrated communications	A shared communications plan and interoperable channels	An out-of-band channel, a command bridge, a status cadence and a list of who hears what, written into the communications plan.
Establishment and transfer of command	Command is established at the start and transferred by briefing	The first qualified person takes command and says so. Handover happens by briefing, is announced, and is logged.
Unified command	Organizations with authority share command through one set of objectives	IT, security, OT, counsel and the business agree one set of objectives and one plan, each keeping authority over its own people.
Unity of command and chain of command	Every person reports to one supervisor, and authority runs in a clear line	Every responder has one boss for the length of the incident, whatever their day-job reporting line.
Accountability	Check-in, assignments, and records of who is where	Everyone working the incident is on the roster with an assignment and a relief time.
Dispatch and deployment	Resources join when requested and dispatched	Help from other teams arrives through the IC or Logistics with an assignment. Nobody freelances.
Information and intelligence management	Collect, analyze and share incident information	Forensic findings and threat intelligence flow through one situation picture, owned by Planning.

If you adopt only three

Name one incident commander out loud, write objectives before tactics, and hand over by briefing. Most of the rest grows from those.

The organization

One commander at the top, a Command Staff beside them for the things only command should own, and a General Staff below who run the work. Positions are filled only when the incident needs them. An empty box on the chart is a job the IC still holds.



The incident organization with cyber units. Dashed boxes are optional. Section colours follow the vest colours many ICS teams wear.

Command

Incident Commander

Owns. Objectives and priorities, approval of the Incident Action Plan, orders for resources beyond the sections' authority, what goes to executives and the public, transfer of command, and the call to demobilize.

First hour. Takes command out loud, sizes up, writes objectives, names an Operations lead, opens communications and sets the first briefing.

Stays off. The keyboard. An IC doing technical work leaves nobody watching the whole incident.

In cyber. The IC needs authority agreed in advance to isolate systems, suspend accounts, activate retainers and spend money. Write it into policy with business-impact and spending limits.

Deputy Incident Commander

Owns. The same qualification as the IC. Runs command while the IC rests, takes delegated work such as coordinating unified command members, and is the default relief at shift change.

Public Information Officer

Owns. Every message leaving the incident organization: executive updates, staff notices, customer and partner statements, media, status pages.

In cyber. Drafts from the incident status summary so every audience gets the same numbers. Clears wording with Legal. Routes attacker contact, extortion notes and leak-site posts to the IC and Legal, unanswered.

Safety Officer

Owns. Authority to stop any action that puts people at risk, and the plan that keeps responders fit to work.

In cyber. Watches three risks. Responder fatigue: shift lengths, rest, handover. Physical processes: where containment touches operational technology, isolating a controller or a segment can stop a process or disable a safety system, so engineering signs off first. Personal safety: staff named in extortion or doxxing get support and, where needed, protection.

Liaison Officer

Owns. The single point of contact for outside parties that are not in command.

In cyber. The outside response firm's engagement lead, the insurer and breach coach, law enforcement, regulators, the ISAC, managed service providers, suppliers, and key customers' security teams. Keeps a log of every commitment made to them.

Legal advisor

Owns. NIMS lets command add technical specialists as advisors. Counsel is the one every cyber incident needs: privilege, notification obligations and their clocks, law enforcement engagement, contracts with responders, and review of anything said outside the organization.

General Staff

Operations Section Chief

Owns. The response work, organized to meet the IAP's objectives. Builds groups, names their supervisors, keeps span of control inside three to seven.

In cyber. This is where the PIVTR-D response loop runs: investigation and scope, containment, eradication and recovery, with an OT group where plant systems are involved. Reports status to Planning on the cadence the IAP sets.

Planning Section Chief

Owns. The situation picture, the Incident Action Plan and the planning cycle, resource status, documentation, and the demobilization plan.

Units. Situation: scope, attack timeline, status summary. Resources: who is assigned, resting, and relieving whom. Documentation: activity logs, decision records, the evidence register index. Demobilization: release plan and check-out.

In cyber. Owns the attack timeline and the incident record, the two documents every later review depends on.

Logistics Section Chief

Owns. Everything responders need to do the work.

In cyber. Clean administrative workstations, break-glass accounts, access for outside responders, forensic licences and storage, spare hardware for rebuilds, the out-of-band channel, the war room, food, and places to rest.

Finance/Admin Section Chief

Owns. Time, cost, procurement, contracts and claims.

In cyber. Tracks every responder hour and outside invoice from the first hour, approves emergency purchases, activates retainers, and keeps the insurer's claim file. Read the cyber policy's notice deadline and panel-vendor terms before the incident, then track them during it.

Intelligence/Investigations

Where it sits. NIMS lets the intelligence and investigations function sit inside Planning, inside Operations, as its own General Staff section, or with the Command Staff.

In cyber. Forensic analysis, threat intelligence and evidence custody. Give it its own section when the investigation is the main effort, when law enforcement works alongside, or when counsel directs the investigation for privilege. Otherwise it stays as the investigation group in Operations.

Branches, groups and task forces

ICS gives the pieces under a section fixed names, so a request for a task force means the same thing to everyone.

Term	In ICS	Cyber example
Branch	Added when a section outgrows its span of control. Functional or geographic	A technical branch and an OT branch under Operations
Division	A geographic or physical area	A data centre, a site, a cloud tenant, a subsidiary
Group	A functional area	Containment group, identity group

Term	In ICS	Cyber example
Task force	Mixed resources under one leader with shared communications	Identity task force: directory engineer, IAM administrator, detection analyst
Strike team	Resources of the same kind and type under one leader	Five endpoint analysts working the rebuild queue
Single resource	One person or item with an assignment	The malware reverse engineer

Who usually fills each seat

Position	Draw from
Incident Commander	Security operations leadership or a senior incident handler trained in ICS
Operations	The incident response lead
Planning	A senior analyst or program manager who writes well under pressure
Logistics	IT operations or service desk leadership
Finance/Admin	A finance partner with procurement authority
Public Information	Corporate communications, paired with a security writer
Liaison	Vendor management or third-party risk
Safety	Health and safety or HR, with OT engineering where plants are involved
Legal advisor	In-house counsel, with outside counsel as needed

> Train two people for every seat you expect to fill. Incidents run longer than one person can.

Sizing the response

NIMS sorts incidents into five complexity types. Type 5 is the smallest. Type 1 is the most complex. The type tells you which positions to fill and whether the plan must be written down.

Type	In NIMS	Cyber example	Written IAP
5	One or two resources, closed within the first operational period	A phishing report with one mailbox affected	No
4	Several resources, one operational period, Command and General Staff not activated	Commodity malware on a handful of endpoints	No. A written objective list is enough
3	Some or all Command and General Staff positions activated, multiple operational periods	Business email compromise with a fraudulent payment, ransomware on one site	Yes, each period
2	Needs resources beyond local capability, most positions filled	Enterprise ransomware with an outside response firm and an insurer	Yes, each period
1	The most complex, all positions filled, national-level resources	A disruption of critical infrastructure with government coordination	Yes, each period

EXAMPLE

If your organization already uses severity levels, map them once, in writing, and publish the mapping.

Severity	Type	Command
SEV 4	5	Analyst in command
SEV 3	4	IC and Operations lead
SEV 2	3	Command and General Staff as needed
SEV 1	2 or 1	Full organization, unified command likely

When to grow

- A supervisor has more than seven people reporting.
- The incident will run past the current operational period.
- An outside response firm, insurer, regulator or law enforcement agency is engaged.
- Customers, the public or the media will hear about it.
- Containment could affect a physical process or anyone's safety.
- Two parts of the organization claim authority over the same systems.
- Business operations are disrupted beyond the technology estate: activate the crisis team as well. See Above the incident.

Order of growth

Add positions in the order the workload usually arrives: an Operations lead, then a Public Information Officer, then Planning with documentation first, then Liaison, then Logistics, then Finance/Admin. Safety joins as soon as shifts run past twelve hours or containment touches a physical process.

When to shrink

Fold positions back as their workload drops, returning their duties to the person above them. The IC announces each change and updates the organization assignment list.

> **Start with three**
>
> For Type 4 incidents, and as the core of every larger one, fill three roles: incident commander, communications lead and operations lead. They are the core roles in Google's incident management system, IMAG, which is built on ICS, so they grow into the full organization without renaming anything. Add Planning when the incident runs past one shift. See Respond and manage.

The planning cycle

An operational period is the time set for carrying out one set of objectives, as written in the Incident Action Plan. Each period gets its own objectives, assignments and briefing. The plan for the next period is written during the current one.

The Planning P. The stem runs once. The loop repeats each operational period.

Setting the period length

Start with twelve-hour periods during active containment, so each shift has its own plan and briefing. Move to twenty-four hours once eradication and recovery are routine, and to longer periods for monitoring. The IC sets the length, and it goes in the IAP.

The meetings

Step	Who	Produces
Initial response and assessment	First responders	Size-up and first actions

Step	Who	Produces
Incident briefing	Outgoing and incoming command	ICS 201
Objectives meeting	IC or unified command	Objectives for the next period (ICS 202)
Command and General Staff meeting	IC with Command and General Staff	Priorities, constraints, decisions
Tactics meeting	Operations, Planning, Logistics, Safety	Work assignments and resource needs
Planning meeting	Command and General Staff	Agreement to the plan
IAP preparation and approval	Planning prepares, IC signs	The Incident Action Plan
Operations briefing	The oncoming shift	Assignments delivered. The period starts
Execute and assess	Operations, with Planning tracking	Status updates, changes flagged to command

A day in twelve-hour periods

EXAMPLE

Time	What happens
06:30	Operations briefing for the day shift
07:00	Day period starts. Night shift hands over and goes to rest
09:00	Executive update from the status summary
11:00	Objectives meeting for the night period
12:00	Command and General Staff meeting
13:00	Tactics meeting
14:30	Planning meeting

Time	What happens
16:00	IAP signed
17:00	Executive update
18:30	Operations briefing for the night shift
19:00	Night period starts. Day shift hands over and goes to rest

What goes in the IAP

- Objectives and command emphasis (ICS 202)
- Organization assignment list (ICS 203) or chart (ICS 207)
- Assignment lists, one per group or division (ICS 204)
- Communications plan (ICS 205)
- Safety and wellbeing message
- Current situation summary

For Type 4 and 5 incidents the incident briefing (ICS 201) is the plan.

Unified command

Unified command is how several parties with authority over the incident run one response. They agree one set of objectives and one plan. Each keeps authority over its own people and budget, and none acts outside the plan without telling the others.

Who sits in it

A party joins unified command when it holds authority or accountability for part of the response.

Party	Joins when	Otherwise
Technology leadership	Systems will be isolated, rebuilt or restored	Supports through Operations
Security leadership	Almost always, for investigation and containment	n/a
OT or engineering	Plant or physical systems are affected or at risk	Advises the Safety Officer
The affected business	Operations, customers or revenue are affected	Receives updates
Counsel	Legal exposure is driving decisions	Legal advisor to command
Managed security provider	It takes containment actions under its contract	Works through Operations
Law enforcement	It holds authority over part of the response, as in some public-sector incidents	Through Liaison

Rules

- One set of objectives and one IAP, approved by every member.
- One Operations Section Chief, whatever the number of members.
- One voice outside the incident, through the Public Information Officer.
- Members sit together, or on one bridge, during planning.
- A member who must act outside the plan says so first and the others hear it before it happens.

Counsel and privilege

If counsel directs the investigation to preserve privilege, record that in the IAP. Documentation, the forensic report and outside responders' deliverables then follow counsel's routing, and Planning keeps the record index to match.

Managed providers

A provider that can isolate hosts or disable accounts in your environment acts inside the plan. Agree in advance which actions it takes on its own authority and which need the Operations Section Chief, then write that list into the IAP so the night shift knows it too.

Insurers

An insurer may require notice within a set time and may direct which response firms and counsel you use. It works through Liaison and Finance/Admin, and its requirements go into the IAP as constraints.

Above the incident

Incident command runs the incident. When the incident reaches the whole organization, NIMS adds three structures above and around it. Each has its own job, and keeping the jobs separate leaves the incident commander free to run the response.

Emergency operations center: the crisis team

An EOC supports incident command and manages consequences away from the incident. In a cyber incident that is the crisis management team: business continuity, operations, finance, HR, facilities and customer operations, led by an executive who is not the incident commander. It runs manual workarounds while systems are down, keeps customers served, finds extra staff and money, and tells the incident commander what the business needs.

Activate it when business operations are disrupted beyond the technology estate, when the incident will run past a day, or when the response needs resources beyond the incident commander's authority.

Multiagency coordination group: the executive decision group

A MAC group is a small set of executives who set policy and priorities when demands exceed resources or several incidents compete. In cyber: the chief executive, general counsel, finance, operations, security and technology leadership, with the board kept informed. They decide what only they can decide: taking a line of business offline, which business unit restores first, public disclosure, any engagement with an extortionist with counsel advising on legal and sanctions exposure, and spending beyond set limits. They leave tactics to the incident commander.

Joint information system: one set of public facts

A JIS coordinates public information across every organization involved. A supplier breach that reaches your customers, or an incident with law enforcement, an insurer and a managed provider involved, puts several communications teams in front of the same audience. The JIS keeps their statements consistent: shared facts, agreed timing, each party speaking for its own part. A joint information center is where those communicators work together, in a room or on a bridge.

How they connect

From	To	What flows
Incident command	Crisis team (EOC)	Status summaries, and resource requests beyond command authority
Crisis team (EOC)	Incident command	Resources, business priorities, decisions within the crisis team's authority

From	To	What flows
Crisis team (EOC)	Executive group (MAC)	Decisions that need executive authority, with options and business impact
Executive group (MAC)	Crisis team and incident command	Priorities, policy decisions, allocation of scarce resources
Every level	Joint information system	Verified facts cleared for release
Joint information system	Every level	Approved statements and their timing

Keep the jobs apart

Watch for executives directing tactics from the crisis room. Give them the decisions only they can make, on a written list, and route everything else to the incident through the incident commander.

Resources

NIMS resource management is how an incident gets the right people and equipment, and gives them back. It rests on three things: describing resources the same way everywhere, knowing who is qualified, and running every request through one process.

Typing

NIMS describes a resource by kind, what it is, and type, how capable it is. Typing lets a request say exactly what is needed and lets a supplier confirm it can deliver. Define your cyber resources the same way before the incident.

EXAMPLE

Resource	Kind	Type 1	Type 2
Incident commander	Personnel	Has commanded a Type 2 or larger incident	Has commanded a Type 3 incident
Forensic analyst	Personnel	Leads host and memory forensics and defends the findings	Collects and processes evidence under supervision
Rebuild strike team	Team	Five technicians with imaging rights and a staging area	Three technicians with imaging rights
Clean administration kit	Equipment	Hardened workstation, break-glass credentials, offline tools	Hardened workstation

Qualification and credentialing

NIMS separates qualifying a person for a position, certifying that they meet the standard, and credentialing them so other organizations can trust it. FEMA's qualification system uses position task books: the tasks a person must show they can do in a role. Write a one-page task book for each seat you fill, and sign it off after an exercise or a real incident.

The resource management process

NIMS runs every incident resource through six steps. Several resources can be at different steps at once.

Step	In a cyber incident
Identify requirements	Operations states what it needs, by kind and type, at the tactics meeting
Order and acquire	Logistics orders from inside the organization, the retainer or mutual aid. Finance/Admin approves the spend
Mobilize	Check-in, assignment, access granted, briefing
Track and report	The Resources unit keeps status: assigned, available, resting, released
Demobilize	Check-out: access revoked, evidence handed over, hardware returned
Reimburse and restock	Invoices paid, insurance claim filed, licences and spares replaced

Mutual aid

Mutual aid agreements let organizations lend each other resources on terms agreed in advance. For cyber, the sources are your sector's ISAC, peer organizations, technology partners, and government support, which varies by sector and state. Agree the terms before you need them: who can ask, what is provided, who pays, and how access and confidentiality work.

Communications and information

Google's guide treats keeping users, stakeholders and leaders informed as just as important as the technical mitigation. Consistent updates at the right level of detail build trust.

What every update answers

1. What is affected: systems, data, locations, people.
2. How bad it is: impact now, and whether it is growing.
3. What people should do: workarounds, password resets, channels to avoid.
4. When it will be mitigated and resolved, or when the next update comes if nobody knows yet.

The communications plan

The communications plan says which channel carries what, who is on it, and how anyone confirms who they are talking to. Planning writes it. Logistics stands it up. The IC approves it with the IAP.

EXAMPLE

Purpose	Primary	Backup	Owner
Command bridge	Standing conference line	Out-of-band chat room	IC
Operations	Out-of-band chat, one room per group	Conference line	Operations
Executive updates	Scheduled call plus written status summary	Phone tree	Public Information
Legal and privileged	Counsel's own channel	Phone	Legal advisor
Outside parties	Named contacts by phone and email outside the affected domain	Liaison's mobile	Liaison

Out of band

Assume the attacker can read corporate email and chat until scoping shows otherwise. Run the response on accounts outside the affected identity provider, verify each member by voice before adding them, and keep the roster somewhere offline. Say out loud when the incident moves channels, and why.

Cadence

Executives get the status summary at fixed times set in the IAP. Every update ends with the time of the next one, including updates with nothing new. A fixed cadence cuts interruptions to responders more than any other single measure.

One voice

Everything leaving the incident goes through the Public Information Officer, drawn from the same status summary and cleared with counsel where it could create legal exposure. Responders asked by anyone outside the organization send them to Public Information or Liaison.

Common operating picture

NIMS calls it the common operating picture: one shared view of the incident that everyone works from. Planning's Situation unit owns it. In cyber it is the status summary, the attack timeline and the scope list, kept in one place, timestamped, and read by incident command, the crisis team and the executives alike. Anyone who needs a number takes it from there.

Writing it down

- Plain language. No acronyms outside the glossary.
- Every time with its timezone.
- Requests and decisions that must survive the incident go on a general message (ICS 213).
- Everyone in a role keeps an activity log (ICS 214).

Taking and handing over command

Taking command

The first qualified person to reach the incident takes command and says so on the channel responders are using: their name, the time, the incident name, and where the command bridge is. They open an activity log and start the incident briefing.

Seniority alone confers no command. A senior leader who arrives gets a briefing, then either takes command through a formal transfer or supports the IC in place.

Transferring command

Command transfers when a more qualified person arrives, when the incident outgrows the current IC, at shift change, or when the IC is too tired to continue.

1. Brief the incoming IC face to face or by voice, using the ICS 201 or the current IAP.
2. Walk the open decisions and every commitment made to outside parties.
3. Agree the effective time.
4. Announce the change to Command and General Staff, all responders, and outside parties who deal with the IC.
5. Log it, with both names and the time.

Shift handover

#	Item
1	Current objectives and progress against each
2	Status of every assignment, with who holds it now
3	Open decisions and who is waiting on them
4	Commitments made to executives, customers, regulators, insurers and law enforcement
5	Safety and wellbeing concerns, including who has worked too long
6	Known unknowns, and what would change the plan
7	Times of the next meetings, briefings and executive updates
8	Where the logs, timeline and evidence register are

#	Item
9	Thirty minutes of overlap between outgoing and incoming people

Fatigue

Set a maximum shift length before the incident, give the Safety Officer authority to enforce it, and roster relief from the first night. The people who stayed up to contain the incident are rarely the right people to make the eradication decisions the next afternoon.

Demobilization

Demobilization releases people and resources in order, with nothing left behind: no open access, no loose evidence, no unbilled hours. Planning writes the demobilization plan as soon as the end is in sight, and the IC approves it.

Release order

Release outside responders and borrowed staff as their objectives close. Keep core responders until eradication is verified. Keep monitoring capacity after that, at the level the recovery plan calls for.

Check-out, per person (after ICS 221)

#	Item
1	Assignment handed to a named person, or closed
2	Activity log submitted to Documentation
3	Notes, evidence and media handed over, with custody recorded
4	Temporary accounts, access and tokens revoked
5	Loaner hardware and licences returned
6	Hours submitted to Finance/Admin
7	Rest before the next shift or return to normal duty

Closing the incident organization

#	Item
1	IC declares the end of the incident, with the time
2	Final status summary issued
3	Emergency changes reviewed and closed or made permanent
4	Outside engagements ended in writing and final invoices requested

#	Item
5	Records consolidated by Documentation and indexed
6	Costs totalled by Finance/Admin, insurer's claim file updated
7	After-action review scheduled, run as the PIVTR-D debrief

Learn

Google's guide makes learning from outages a core tenet and notes that outages left unchecked tend to come back and pile up. Its main tool is the blameless postmortem. NIMS reaches the same place through the after-action report and improvement plan, the AAR/IP format of the Homeland Security Exercise and Evaluation Program.

Start while it is fresh

Start the write-up as soon as the incident is resolved. Planning already holds the raw material: the activity logs, the timeline, the Incident Action Plans, the decision records and the status summaries. The review turns that record into an explanation.

Blameless

Everyone in the response acted in good faith on what they knew at the time. Findings go to systems, procedures and training. Record the decisions and the information behind them, and leave individual names out of the causes.

Review the management as well as the fix

The technical cause is examined in the PIVTR-D debrief. Review the incident management alongside it, area by area.

Area	Questions
Detection	How long from first sign to someone taking command? What would have paged sooner?
Command	Was command clear from the start? How many handovers, and did each carry the open decisions?
Planning	Were objectives written before tactics? Did each period have a plan, and did the work follow it?
Communications	Did every audience get the same facts on schedule? Did anything contradict or leak?
Operations	Did span of control hold? Did anyone work without an assignment?
Logistics	Did responders have access, tools and rest when they needed them?
Finance/Admin	Were hours, costs and insurer deadlines tracked from the first hour?

Area	Questions
Safety	Did anyone work past the shift limit? Did containment put a physical process at risk?

Improvement plan

Each corrective action gets one owner, a due date agreed with the people who will staff and fund it, and a way to confirm it is done. Actions go into the owning team's backlog and are tracked there until closed. Share the review widely inside the organization.

Across incidents

Once reviews are routine, keep their findings in one structured register. Findings that recur across incidents show where larger investment belongs: a detection gap that keeps adding hours, a handover that keeps dropping decisions, a supplier that keeps being the way in.

After-action report and improvement plan (after HSEEP AAR/IP)

```
AFTER-ACTION REPORT AND IMPROVEMENT PLAN (after HSEEP AAR/IP)
Incident name and number:
Dates, first sign to close:
Incident type at peak:
Prepared by:                  Reviewed by:

1. Summary
   What happened, in five sentences or fewer.

2. Timeline
   First sign, command established, contained, eradicated, recovered, closed.

3. What worked
   Strength      Why it worked      How we keep it

4. What to improve
   Area      Observation      Cause      Recommendation

5. Improvement plan
   Action      Owner      Due      How we confirm it is done      Status

6. Hours and costs
   Responder hours:        Outside costs:        Insurance claim status:

7. Distribution
   Who receives this report:
```

Forms and templates

ICS forms exist so that anyone joining the incident can read its state in minutes. These are the ones a cyber incident uses most, cut down to plain text so they paste into a ticket, a chat room or a document. FEMA publishes the full set in its ICS forms booklet. The after-action report and improvement plan is on Learn.

Form	Name	Use
ICS 201	Incident briefing	The first plan, and the briefing for any transfer of command
ICS 202	Incident objectives	The objectives and command emphasis for one period
ICS 203	Organization assignment list	Who holds which position this period
ICS 204	Assignment list	One per group or division: the work, the people, the instructions
ICS 205	Communications plan	Channels, owners and verification, out of band
ICS 209	Incident status summary	The executive update, and the source for every message
ICS 213	General message	Written requests and decisions
ICS 214	Activity log	Everyone in a role keeps one
None	Transfer of command	The handover record
ICS 221	Demobilization check-out	Release of one person

ICS 201. Incident briefing

```
INCIDENT BRIEFING (after ICS 201)
Incident name:                    Incident number:
Prepared by:                      Date, time, timezone:
Incident commander:

1. Situation
   What happened, what is affected, what is known, what is not.

2. Current objectives
   1.
   2.
   3.

3. Actions taken so far
   Time      Action      By

4. Current organization
   IC:
   Operations:
   Planning:
   Public Information:
   Liaison:
   Legal advisor:

5. Resources assigned and ordered
   Resource      Assigned to      Status

6. Safety and wellbeing
   Hours worked, physical process risks, personal safety concerns.

7. Next briefing:
```

ICS 202. Incident objectives

```
INCIDENT OBJECTIVES (after ICS 202)
Incident name:
Operational period: from                    to
Objectives, each with an outcome, a measure and a time:
  1.
  2.
  3.
Command emphasis (priorities, constraints, risk tolerance):
Decisions made by command this period:
Safety and wellbeing message:
Attached: organization list, assignment lists, communications plan, situation summary
Approved by (IC or each unified command member):          Time:
```

ICS 203. Organization assignment list

```
ORGANIZATION ASSIGNMENT LIST (after ICS 203)
Operational period:
Command
  Incident commander:
  Deputy:
  Public Information Officer:
  Safety Officer:
  Liaison Officer:
  Legal advisor:
Operations Section Chief:
  Group, supervisor, members:
Planning Section Chief:
  Situation unit:
  Resources unit:
  Documentation unit:
Logistics Section Chief:
Finance/Admin Section Chief:
Intelligence/Investigations (if separate):
Unified command members (if used):
```

ICS 204. Assignment list

```
ASSIGNMENT LIST (after ICS 204)
Operational period:
Group or division:               Supervisor:
Members:
Work assignment, and the objective each task serves:
Special instructions (change windows, systems not to touch, evidence handling):
Status to Planning at:           via:
Channels: primary            backup
Prepared by (Planning):          Approved by (Operations):
```

ICS 205. Communications plan

```
COMMUNICATIONS PLAN (after ICS 205)
Treat corporate email, chat and identity as compromised until scoping shows otherwise.
Purpose              Primary            Backup             Owner
Command bridge
Operations
Executive updates
Legal, privileged
Outside parties
Roster kept at (offline):
How members verify each other:
Status cadence:
```

ICS 209. Incident status summary

```
INCIDENT STATUS SUMMARY (after ICS 209)
As of (date, time, timezone):
Incident name and number:          Type:
Incident commander:
What is affected:
How bad it is (impact now, and whether it is growing):
What people should do now:
When it will be mitigated and resolved, if known:
Scope: systems affected          confirmed          suspected
Containment status:
Objectives this period, and progress on each:
Outside parties engaged:
Notifications made, and due:
Decisions needed from leadership:
Next update:
```

ICS 213. General message

```
GENERAL MESSAGE (after ICS 213)
To:                    Position:
From:                  Position:
Subject:
Date, time, timezone:
Message:

Reply:

Replied by:            Date, time:
```

ICS 214. Activity log

```
ACTIVITY LOG (after ICS 214)
Name:                  Position:              Operational period:
Time (with timezone)     Activity, decision or observation
```

Transfer of command

```
TRANSFER OF COMMAND
Outgoing IC:                      Incoming IC:
Effective (date, time, timezone):
Briefed from: ICS 201 / current IAP
Covered:
  Situation and scope
  Objectives and progress
  Organization, and who is on shift
  Open decisions
  Commitments made to outside parties
  Safety and wellbeing
  Next meetings and updates
Announced to: command staff / general staff / all responders / outside parties
Logged by:
```

ICS 221. Demobilization check-out

```
DEMOBILIZATION CHECK-OUT (after ICS 221)
Name:                  Position:             Released at:
Assignment handed to:
Activity log to Documentation:          yes / no
Evidence and notes handed over, custody recorded:          yes / no
Temporary access revoked:          yes / no
Hardware and licences returned:          yes / no
Hours to Finance/Admin:          yes / no
Rest before next duty:
Released by:
```

Glossary

Common terminology is the first of the NIMS management characteristics for a reason. Agree these words before the incident.

Term	Meaning
Incident Commander (IC)	The one person with overall authority for the incident
Unified command (UC)	Several parties with authority sharing command through one set of objectives and one plan
Command Staff	Public Information, Safety and Liaison Officers, plus advisors such as counsel, reporting to the IC
General Staff	The section chiefs: Operations, Planning, Logistics, Finance/Admin, and Intelligence/Investigations if separate
Section	A major functional area of the organization, led by a chief
Branch, division, group	Subdivisions of a section: branch by function or area, division by area, group by function
Task force	Mixed resources under one leader with shared communications
Strike team	Resources of the same kind and type under one leader
Operational period	The time set for carrying out one set of objectives, as written in the IAP
Incident Action Plan (IAP)	The written plan for one operational period
Objective	An outcome with a measure and a time
Span of control	The number of people one supervisor manages
Incident command post	Where command operates. In cyber, usually the war room or command bridge
Check-in	Recording that a person has joined the incident, with their assignment

Term	Meaning
Out of band	Communications that do not depend on systems the attacker may control
Contained	Agree the definition in advance. PIVTR-D uses: network, process and log channels all show attacker activity stopped
Demobilization	The orderly release of people and resources
Transfer of command	Handing command to another person by briefing, announced and logged
Three Cs	Coordinate, communicate, control: the aims Google's ICS-based system organizes around
Communications lead	Google's name for the role NIMS calls the Public Information Officer
Operations lead	Google's name for the role NIMS calls the Operations Section Chief
Incident management team (IMT)	A rostered group of ICS-qualified people who deploy to manage an incident
AAR/IP	After-action report and improvement plan, the review format of the Homeland Security Exercise and Evaluation Program
Emergency operations center (EOC)	Where staff coordinate support to incident command and manage wider consequences. In cyber, the crisis management team
Multiagency coordination group (MAC group)	Executives who set policy and priorities across incidents. In cyber, the executive decision group
Joint information system (JIS)	The processes that keep public information consistent across every organization involved
Joint information center (JIC)	Where communicators from each organization work together
Resource typing	Describing a resource by kind and by capability, so requests and offers match
Position task book	The tasks a person must show they can do to qualify for an incident position

Term	Meaning
Mutual aid	Sharing resources between organizations on terms agreed in advance
Common operating picture	One shared, timestamped view of the incident that every level works from

Sources and licence

This guide adapts the National Incident Management System, Third Edition, published by FEMA in October 2017, and the Incident Command System forms, to cybersecurity. Both are works of the United States government. The three components, the four command and coordination structures, the fourteen management characteristics and the resource management process are summarized from NIMS.

The three-stage structure, the three Cs and the three core roles take their cue from Google's Incident Management Guide, written by Adam Crume, Alex Cepoi, Chelsea Granados, Roxana Loza, Steve McGhee, Svetlana Gites, Trevor Mattson-Hamilton and Vrai Stacey, and from the Managing Incidents chapter of ***Site Reliability Engineering***. Both are summarized and credited here. No text from them is reproduced.

The after-action format follows the AAR/IP of the Homeland Security Exercise and Evaluation Program.

Not published by, endorsed by, or affiliated with FEMA, the Department of Homeland Security or Google.

Adapted from the National Incident Management System, Third Edition (FEMA, 2017). Cyber adaptation, examples and templates by Habib Tora, licensed under CC BY 4.0. Not published by, endorsed by, or affiliated with FEMA or the Department of Homeland Security. Structure after Google's SRE Incident Management Guide. Companion to PIVTR-D.