2 RESPOND AND MANAGE

Position checklists

Each ICS seat has a job aid, grouped by when you use it: on taking the seat, every operational period, and before handing over. Print the page for the war room, or copy any list into the incident channel as a Markdown checklist. The seats are described in The organization, and the forms in Forms.

Incident Commander

REPORTS TO
The executive who delegated authority for the incident, the Agency Administrator in NIMS terms

FILL THE SEAT
Every incident. At Type 5 it is often the analyst who found it. From Type 2, add a Deputy Incident Commander, or a second Incident Commander for alternate periods.

FORMS
Prepares the ICS 201. Approves the ICS 202, the Incident Action Plan and the ICS 209.

On taking the seat

#	Item
☐ 1	Take command out loud: your name, the time, the incident name and where the command bridge is. Open your activity log (ICS 214).
☐ 2	If someone was in command before you, take a briefing from them, using the ICS 201 if one exists.
☐ 3	Open a command bridge and an out-of-band channel, and record both in the ICS 205. Treat email, chat and identity as visible to the attacker until scoping shows otherwise.
☐ 4	Size up: what happened, what is affected, what is still happening and what is unknown.
☐ 5	Set up to three objectives, each with an outcome, a measure and a time. Examples are in Writing objectives.
☐ 6	Name an Operations Lead, or an Operations Section Chief from Type 3, and hand over the technical work. Stay off the keyboard.
☐ 7	Decide the incident type, 5 to 1, with the type chooser, and fill the positions it calls for.
☐ 8	Confirm your authority limits, and who approves anything above them.

#	Item
☐ 9	Tell counsel if personal data, regulators, law enforcement, extortion or insurance may be involved. The clocks are in notification deadlines.
☐ 10	Set the times of the first briefing and the first executive update, using the update schedule for the severity.
☐ 11	Write the incident briefing (ICS 201) before the first briefing.
☐ 12	Check hours: who has been awake since when, and who relieves them. Record hazards and rest rules in the ICS 208.

Every operational period

#	Item
☐ 1	Run the objectives meeting and approve the ICS 202.
☐ 2	Approve the Incident Action Plan before the operations briefing.
☐ 3	Approve the ICS 209 before it goes to executives.
☐ 4	Approve resource orders beyond the sections' authority.
☐ 5	Check span of control, and add or fold positions as the workload changes.
☐ 6	Review hours worked with the Safety Officer and roster relief.

Before handing over

#	Item
☐ 1	Brief the incoming IC by voice from the ICS 201 or the current IAP.
☐ 2	Walk every open decision and every commitment made to outside parties.
☐ 3	Agree the effective time, announce the change, and log it with both names.

Deputy Incident Commander

REPORTS TO	FILL THE SEAT	FORMS
The Incident Commander	From Type 2, or sooner when the Incident Commander needs relief across operational periods or has command work to hand off. The deputy must be able to take over as Incident Commander at any time. A second Incident Commander who commands alternate periods, as in the worked example, covers the relief use.	Keeps an ICS 214. Reads each ICS 201, 202 and 209 when it is issued, and uses the Incident Commander's forms while in command.

Owns. The command tasks the Incident Commander delegates, and command itself while relieving the Incident Commander. ICS gives a deputy three uses.

One is specific tasks the Incident Commander assigns. Another is relief in command, for example for the next operational period. The third is representing a party that has, or may later have, authority over part of the incident.

On taking the seat

#	Item
☐ 1	Take a briefing from the Incident Commander, using the ICS 201 or the current IAP. Open your activity log (ICS 214).
☐ 2	Agree which tasks you own and which decisions stay with the Incident Commander, and record the split in both activity logs.
☐ 3	Read the delegation of authority, so you know the limits that apply when you take command.
☐ 4	If you are the relief in command, agree which operational periods you command and the time of each transfer.
☐ 5	If you represent another party, agree with the Incident Commander which of its decisions you can make on the spot and which go back to it.
☐ 6	Ask Planning to add you to the ICS 203, and announce your role on the command bridge.

Every operational period

#	Item
☐ 1	Run the tasks the Incident Commander delegated, such as coordinating unified command members, and report on each at the objectives meeting.
☐ 2	Attend the objectives meeting and the planning meeting, so you can explain every decision in the IAP when you take command.
☐ 3	Keep a list of open decisions, with who is waiting on each and by when.
☐ 4	Before you relieve the Incident Commander, take the handover briefing and follow Transferring command. While in command, work from the Incident Commander job aid.
☐ 5	Track your hours and the Incident Commander's, and tell the Safety Officer before either of you reaches the shift limit.

Before handing over

#	Item
☐ 1	Hand each delegated task back to the Incident Commander or to a named person, with its status.
☐ 2	If you are in command, transfer it on the transfer of command record, announce it, and log it with both names.
☐ 3	Brief the incoming deputy by voice on the delegated tasks and the open decisions.

Built from FEMA's ICS 300 review document (March 2018), which gives a deputy these three uses and requires a deputy to be able to take over the primary role.

Public Information Officer

REPORTS TO	FILL THE SEAT	FORMS
The Incident Commander	As soon as anyone outside the response team has to be told.	Drafts from the ICS 209 and logs on an ICS 214.

On taking the seat

#	Item
☐ 1	Get the current status summary and the list of who already knows about the incident.
☐ 2	List every audience: executives, staff, customers, partners, media, and regulators through counsel.
☐ 3	Agree with the IC who approves each kind of message, and with counsel which ones need legal review.
☐ 4	Take the update cadence from the update schedule for the severity, and put the times in the IAP.
☐ 5	Prepare an interim statement before anyone asks for one, on PIVTR-D T18.
☐ 6	Tell staff where to send questions from outside the organization.

Every operational period

#	Item
☐ 1	Draft every update from the current ICS 209 so every audience gets the same facts.
☐ 2	Make each update say what is affected, how bad it is, what people should do, and when it will be fixed or the next update is due.
☐ 3	Send attacker contact, extortion notes and leak-site posts to the IC and counsel, unanswered.
☐ 4	Agree wording and timing with the other parties' communicators through the joint information system.
☐ 5	Log every message sent, with the time, the audience and who approved it.

Before handing over

#	Item
☐ 1	Hand over the message log and every promised update time.
☐ 2	List open media and customer questions, with who is waiting on each.

Safety Officer

REPORTS TO
The Incident Commander

FILL THE SEAT
When the incident runs past one operational period, or when containment could touch a physical process.

FORMS
Writes the safety message (ICS 208) and the IAP safety analysis (ICS 215A).

On taking the seat

#	Item
☐ 1	Confirm your authority to stop any action that puts people at risk, and tell Operations you have it.
☐ 2	Get the roster with the hours worked by everyone on the response.
☐ 3	List every containment action that could affect a physical process or a safety system, and require engineering sign-off before it runs.
☐ 4	Ask HR and physical security to support any staff named in extortion or doxxing.

Every operational period

#	Item
☐ 1	Enforce the maximum shift length and the relief roster.
☐ 2	Review the tactics at the tactics meeting for risk to people and to physical processes.
☐ 3	Write the safety and wellbeing message for the IAP.
☐ 4	Record every action you stopped, and why.

Before handing over

#	Item
☐ 1	Name everyone at or near the hours limit.

#	Item
☐	2 Hand over every open safety concern and every pending engineering sign-off.

Liaison Officer

REPORTS TO	FILL THE SEAT	FORMS
The Incident Commander	When outside parties are engaged.	Logs on an ICS 214 and records requests on ICS 213 general messages.

On taking the seat

#	Item
☐ 1	List every outside party and one named contact at each: the response firm, the insurer and breach coach, law enforcement, managed providers, suppliers, the ISAC, and regulators through counsel.
☐ 2	Tell the IC which of them have authority over part of the response and belong in unified command.
☐ 3	Give each party a single contact point on the incident, which is you.
☐ 4	Agree with counsel what may be shared with each party.

Every operational period

#	Item
☐ 1	Brief outside parties at the times the IAP sets.
☐ 2	Bring their requests and constraints to the Command and General Staff meeting.
☐ 3	Log every commitment made to them, with a date and an owner.
☐ 4	Carry evidence and preservation requests to suppliers on PIVTR-D T19, and log each with its due date.

Before handing over

#	Item
☐ 1	Hand over the commitment log and every pending request.

Legal advisor

REPORTS TO
The Incident Commander

FILL THE SEAT
When personal data, regulators, law enforcement, extortion or insurance may be involved.

FORMS
Records privilege routing in the IAP.

On taking the seat

#	Item
☐ 1	Decide whether counsel will direct the investigation to preserve privilege, and have it recorded in the IAP.
☐ 2	List every notification obligation, with its deadline and what starts its clock, starting from Notification deadlines and the PIVTR-D sector pages. Work each regulator's notice on T17.
☐ 3	Confirm engagement terms for outside responders.
☐ 4	Issue preservation instructions for evidence and records.

Every operational period

#	Item
☐ 1	Review every message leaving the incident that could create legal exposure.
☐ 2	Track notification deadlines and advise the IC before each one falls due.
☐ 3	Advise on law enforcement engagement and on any contact from the attacker.

Before handing over

#	Item
☐ 1	Hand over the deadline list, the privilege routing and any open advice.

Operations Section Chief

REPORTS TO
The Incident Commander

FILL THE SEAT
Every incident above Type 5. At Type 4 the seat is the Operations Lead, who becomes the Operations Section Chief at Type 3.

FORMS
Builds the ICS 215 at the tactics meeting, and guides the ICS 204 assignment lists, which the resources unit in Planning prepares.

On taking the seat

#	Item
☐ 1	Get the objectives and the current scope from the IC.
☐ 2	Organize the work into groups, each with a named supervisor and three to seven people.
☐ 3	Agree with the IC which containment actions need approval before they run.
☐ 4	Set the cadence for status reports to Planning.
☐ 5	Request people, tools and access through Logistics, on the resource request.

Every operational period

#	Item
☐ 1	Bring tactics and resource needs to the tactics meeting.
☐ 2	Deliver assignments at the operations briefing, one ICS 204 per group.
☐ 3	Run the PIVTR-D response loop and report each pass to Planning.
☐ 4	Tell the IC at once about any change that affects the objectives.

Before handing over

#	Item
☐ 1	Hand over the status of every group, the actions in progress and any evidence in hand.

Division/Group Supervisor

REPORTS TO	FILL THE SEAT	FORMS
The Operations Section Chief, or a Branch Director once Operations has branches. At Type 4, the Operations Lead.	Every group or division Operations sets up, usually from Type 4. Each supervisor leads three to seven people.	Receives one ICS 204 at the operations briefing and works from it. Keeps an ICS 214.

Owns. One part of the IAP, as written on one ICS 204: the work, the people doing it, their safety, and reports on progress. A group splits the work by function, such as the Containment, Rebuild and Investigation groups in the worked example.

A division splits it by place, such as a data center or a cloud tenant. Division and group supervisors have the same level of authority.

On taking the seat

#	Item
☐ 1	Take a briefing from the Operations Section Chief or Branch Director. Read your ICS 204 and the objectives on the ICS 202 that it serves.
☐ 2	Attend the operations briefing, and raise anything on the ICS 204 your group cannot deliver in the period.
☐ 3	Confirm every member has checked in with the Resources unit and has the access and tools the work needs.
☐ 4	Brief the members on each task, the objective it serves, the special instructions and the channels.
☐ 5	Confirm which actions need approval before they run, and who gives it.
☐ 6	Agree hand-offs with the supervisors of the groups your work depends on, for example when the Investigation group dates the backups the Rebuild group may restore.

Every operational period

#	Item
☐ 1	Assign each task on the ICS 204 to named members, and move people between tasks as the work changes.

#	Item
☐ 2	Keep members to the special instructions: systems not to touch, change windows and evidence handling.
☐ 3	Report progress and the status of your people at the times on the ICS 204, through the channel it names.
☐ 4	Coordinate with the supervisors of adjacent groups and divisions before anyone touches a system you share.
☐ 5	Request more people or tools through the Operations Section Chief or Branch Director.
☐ 6	Report at once anything that changes the plan: new hosts or accounts in scope, a containment action that failed, or a responder too tired or unwell to continue.
☐ 7	Solve the group's own access, license and workstation problems, and pass the rest to Logistics.
☐ 8	Send anyone at the shift limit to rest, and tell the Safety Officer.

Before handing over

#	Item
☐ 1	Debrief the Operations Section Chief or Branch Director before you leave the shift.
☐ 2	Brief the incoming supervisor face to face or by voice: each task's status, actions in progress, evidence in hand, and hazards.
☐ 3	Hand your ICS 214 to Documentation.

Built from FEMA's Division/Group Supervisor position checklist (February 10, 2012) and position task book (July 2019), the NWCG incident position description, and NIMS (2008) Appendix B. Appendix B gives division and group supervisors the same level of authority.

Planning Section Chief

REPORTS TO
The Incident Commander

FILL THE SEAT
When the incident runs past one shift.

FORMS
Prepares the ICS 202, 209 and the IAP. Its units prepare the ICS 203, 204, 211 and 221, and keep the open action tracker.

On taking the seat

#	Item
☐ 1	Start the incident record and the attack timeline, or take them over from whoever started them.
☐ 2	Stand up the situation, resources and documentation units as the workload needs.
☐ 3	Publish the meeting schedule for the operational period.
☐ 4	Check in everyone working the incident on the ICS 211, with an assignment and a relief time.

Every operational period

#	Item
☐ 1	Prepare the ICS 202 after the Command and General Staff meeting, for the IC to approve.
☐ 2	Assemble the IAP: the ICS 202, 203 and 204s, the communications plan and the safety message.
☐ 3	Prepare the ICS 209 on the cadence the IAP sets.
☐ 4	Keep the common operating picture current, timestamped and in one place.
☐ 5	Collect the activity logs from every position.
☐ 6	Start the demobilization plan as soon as the end is in sight.

Before handing over

#	Item
☐ 1	Hand over the situation, the planning products in progress and the meeting schedule.

Situation Unit Leader

REPORTS TO	FILL THE SEAT	FORMS
The Planning Section Chief	When the Planning Section Chief stands up the unit, as the workload needs. Until then the Planning Section Chief does this work.	Drafts the ICS 209 for the Planning Section Chief. Keeps the attack timeline, the scope list and an ICS 214.

Owns. The common operating picture: the status summary, the attack timeline and the scope list, in one place and timestamped. Also the analysis and predictions that command and Operations ask for, and any Technical Specialists assigned to the unit.

On taking the seat

#	Item
☐ 1	Take a briefing from the Planning Section Chief. Get the ICS 201, the current IAP and the incident record, PIVTR-D T1.
☐ 2	Take over the attack timeline and the scope list, and publish them where everyone on the response can read them, outside the affected identity provider.
☐ 3	List your sources and when each reports: every group's status reports, findings from Intelligence/Investigations, the activity logs, and outside parties through Liaison.
☐ 4	Agree the ICS 209 times with the Planning Section Chief, from the IAP and the executive update schedule.
☐ 5	Brief any Technical Specialists assigned to the unit on the questions they are answering, and when each answer is due.

Every operational period

#	Item
☐ 1	Update the timeline and the scope list as reports arrive. Record each entry with its time, time zone and source.
☐ 2	Count a host or account as confirmed only with evidence, and list the rest as suspected.
☐ 3	Interview supervisors coming off shift about what they found and how well their tactics worked.

#	Item
☐ 4	Draft the ICS 209 from the timeline and the scope list before each executive update, and give it to the Planning Section Chief.
☐ 5	Give the situation briefing at the planning meeting and the operations briefing.
☐ 6	Give command and Operations a prediction at set times or on request, for example which hosts are likely to be hit next, or when restores will finish.

Before handing over

#	Item
☐ 1	Brief your relief on the current situation and anything unusual.
☐ 2	Hand over the timeline, the scope list, the next ICS 209 time, and every open question with who is answering it.
☐ 3	Hand your ICS 214 to Documentation.

Built from FEMA's Situation Unit Leader position checklist (February 10, 2012), the NWCG incident position description, and the FEMA ICS forms booklet. The booklet names the Situation Unit Leader as the usual preparer of the ICS 209.

Resources Unit Leader

REPORTS TO
The Planning Section Chief

FILL THE SEAT
When the Planning Section Chief stands up the unit, as the workload needs, and at the latest before an outside response firm arrives. Until then the Planning Section Chief does this work.

FORMS
Runs check-in on the ICS 211. Prepares the ICS 203 and, with the Operations Section Chief, the ICS 204s. Keeps an ICS 214.

Owns. Check-in, the master roster, and the status of every person and resource on the incident: assigned, available, resting or released.

On taking the seat

#	Item
☐ 1	Take a briefing from the Planning Section Chief. Get the resource list on the ICS 201 and the current ICS 203.
☐ 2	Open check-in on the ICS 211 at every place responders join: the command bridge, the war room and the out-of-band channel.
☐ 3	Check in everyone already working, with assignment, supervisor, relief time, when they last slept, and any access granted, with its end date.
☐ 4	Start the master roster and a status board showing who is assigned, available, resting or released.
☐ 5	Get status from the people who have it: the Operations Section Chief, each supervisor, the first Incident Commander, and Logistics for people and tools on order.

Every operational period

#	Item
☐ 1	Record every arrival, reassignment, rest period and release as it happens.
☐ 2	Bring the roster to the tactics meeting: who is available for the next period, who needs relief, and which skills are missing.

#	Item
☐ 3	Prepare the ICS 203 and, with the Operations Section Chief, one ICS 204 per group or division for the IAP.
☐ 4	Tell the Safety Officer about anyone near the shift limit and any seat without a named relief.
☐ 5	Give Logistics and Finance/Admin every arrival and departure, so access and recorded hours match the roster.
☐ 6	Tell the Planning Section Chief whose work is closing, for the demobilization plan.

Before handing over

#	Item
☐ 1	Brief your relief on the roster, pending arrivals and releases, and anything unusual.
☐ 2	Hand over the master roster, the status board and the check-in lists.
☐ 3	Hand your ICS 214 to Documentation.

Built from FEMA's Resources Unit Leader position checklist (February 10, 2012), the NWCG incident position description, and the FEMA ICS forms booklet. The booklet names the Resources Unit Leader as the usual preparer of the ICS 203 and, with the Operations Section Chief, the ICS 204.

Documentation Unit Leader

REPORTS TO	FILL THE SEAT	FORMS
The Planning Section Chief	When the Planning Section Chief stands up the unit, as the workload needs, and at the start of any incident that may lead to litigation, a regulator's inquiry or an insurance claim. Until then the Planning Section Chief does this work.	Files every ICS form and PIVTR-D record, and collects every position's ICS 214.

Owns. The incident files: every plan, form, log, decision record and report, checked and filed, and the index of the evidence register.

On taking the seat

#	Item
☐ 1	Take a briefing from the Planning Section Chief. Ask the Legal advisor whether counsel directs the investigation, and how privileged material is labeled and routed.
☐ 2	Set up the incident files where the attacker cannot read them, with access limited to the response and counsel.
☐ 3	Lay out the files: one folder per operational period for the IAP and its forms, and one each for the incident record, decisions, general messages, activity logs and the evidence register index.
☐ 4	Collect what exists: the ICS 201, any transfer of command records, and the activity logs and notes kept so far.
☐ 5	Apply the Legal advisor's preservation instructions to the incident files.

Every operational period

#	Item
☐ 1	Send the approved IAP to everyone on its distribution list, and file the signed copy.
☐ 2	Accept and file every form, log and report on the day it arrives.

#	Item
☐ 3	Check each record for names, times with time zones, and approvals, and return errors to the author.
☐ 4	Keep the decision register: one numbered entry per decision, and each reversed entry marked with the number that replaced it.
☐ 5	Collect the ICS 214 from every position at the end of the period.
☐ 6	Keep the evidence register index in step with the register Intelligence/Investigations keeps.
☐ 7	Answer requests for records along counsel's routing, and log what went to whom.

Before handing over

#	Item
☐ 1	Brief your relief on the file layout, missing records and open requests.
☐ 2	At the end of the incident, index the files and give the complete set to the Planning Section Chief.
☐ 3	File your own ICS 214.

Built from FEMA's Documentation Unit Leader position checklist (February 10, 2012) and the NWCG incident position description.

Logistics Section Chief

REPORTS TO	FILL THE SEAT	FORMS
The Incident Commander	When responders need access, tools or facilities the response team cannot arrange for itself.	Prepares the ICS 205 through the communications unit.

On taking the seat

#	Item
☐ 1	Stand up the out-of-band channel and the command bridge, with accounts outside the affected identity provider.
☐ 2	Provide clean administrative workstations and break-glass access.
☐ 3	Arrange access for outside responders, with an end date on every account.
☐ 4	Set up the war room, physical or virtual.

Every operational period

#	Item
☐ 1	Fill the resource requests from the tactics meeting.
☐ 2	Have the communications unit prepare the ICS 205 and give it to Planning for the IAP.
☐ 3	Track forensic licenses, evidence storage and rebuild hardware.
☐ 4	Arrange food, transport and places to rest.

Before handing over

#	Item
☐ 1	Hand over open orders, every temporary account and all hardware on loan.

Finance/Admin Section Chief

REPORTS TO	FILL THE SEAT	FORMS
The Incident Commander	When outside costs, contracts or insurance claims begin.	Keeps the time and cost records.

On taking the seat

#	Item
☐ 1	Open a cost code for the incident and record responder hours from the first hour.
☐ 2	Read the cyber insurance policy's notice deadline and panel-vendor terms, and tell the IC and Liaison.
☐ 3	Confirm who can approve emergency purchases, and up to what amount.
☐ 4	Activate the retainers the IC has approved, with the retainer script.

Every operational period

#	Item
☐ 1	Record hours for everyone on the roster.
☐ 2	Approve emergency purchases within your authority, and route the rest to the IC.
☐ 3	Update the cost summary and the insurer's claim file.

Before handing over

#	Item
☐ 1	Hand over costs to date, open purchases and invoices, and the claim status.

Intelligence/Investigations

REPORTS TO
The Incident Commander

FILL THE SEAT
When the investigation is the main effort, law enforcement works alongside, or counsel directs the investigation for privilege.

FORMS
Keeps the evidence register. Findings follow counsel's routing when privilege applies.

On taking the seat

#	Item
☐ 1	Agree with counsel how findings are routed and recorded.
☐ 2	Take over the evidence register, and confirm chain of custody for everything collected so far. Collection steps are in PIVTR-D evidence collection.
☐ 3	Set priorities for forensic analysis with the IC.

Every operational period

#	Item
☐ 1	Feed findings into Planning's situation picture on the cadence the IAP sets.
☐ 2	Share threat intelligence with Operations for scoping.
☐ 3	Keep the evidence register current.

Before handing over

#	Item
☐ 1	Hand over open analysis, and log every custody transfer.

Technical Specialist

REPORTS TO

Whoever needs the skill, most often the Planning Section Chief. In the Situation unit, the Situation Unit Leader.

FILL THE SEAT

When the response needs a skill nobody on the roster has. Order outside specialists through Logistics. The Incident Commander approves orders beyond the sections' authority.

FORMS

Checks in on the ICS 211 and keeps an ICS 214. Puts advice that a decision depends on in writing, on an ICS 213.

Owns. Advice and work in one specialty. ICS places Technical Specialists in the Planning Section or wherever their skills are needed, with no fixed position in the structure.

Cyber specialists

Specialist	Reports to	Rules
Forensic analyst from a response firm	Intelligence/Investigations, or the Investigation group supervisor while the investigation sits in Operations	Works to the analysis priorities Intelligence/Investigations sets with the Incident Commander. Hashes every image and enters it in the evidence register. Findings follow counsel's routing when privilege applies.
Ransomware negotiator	Intelligence/Investigations, or Planning while the investigation sits in Operations. See Command by incident type	Contacts the attacker only after the executive decision group approves engagement, with counsel advising on legal and sanctions exposure. Sends each message only after the Incident Commander approves it and the Legal advisor reviews it. Logs every message sent and received. Passes the attacker's claims to Intelligence/Investigations to verify.
Cloud provider engineer	The group working the affected tenant, or Planning when the incident is on the provider's side	Works through the open support case. Gives the case number, the provider's findings and its next update time at each status report. Requests to the provider's account team go through Liaison.
OT engineer	The OT group or OT branch in Operations, advising the Safety Officer	Reviews every containment action on plant systems before it runs, and gives or withholds engineering sign-off. Tells the Safety Officer about any action that could stop a process or disable a safety system.

On taking the seat

#	Item
☐ 1	Check in with the Resources unit on the ICS 211, and get access with an end date through Logistics.
☐ 2	Take a briefing from the person you report to: the question to answer, the deadline, and who acts on your answer.
☐ 3	Agree with the Legal advisor what you may record and share, and where your findings go.
☐ 4	Confirm what you may do in the environment on your own, and what needs approval from the Operations Section Chief first.
☐ 5	Use only the channels in the communications plan (ICS 205).

Every operational period

#	Item
☐ 1	Report findings or advice at the times your supervisor sets, marking what is confirmed, what is suspected, and how sure you are.
☐ 2	Attend the tactics or planning meeting when your specialty shapes the plan.
☐ 3	Log every action you take in the environment, with the time, on your ICS 214.
☐ 4	Enter every item of evidence you collect in the evidence register, with custody recorded.

Before handing over

#	Item
☐ 1	Hand findings, open questions and work in progress to a named person, in writing.
☐ 2	Hand evidence and notes to Intelligence/Investigations, with custody recorded.
☐ 3	Check out on the ICS 221: access revoked, hardware returned, hours to Finance/Admin.
☐ 4	Hand your ICS 214 to Documentation.

Built from FEMA's ICS 300 review document (March 2018), which places Technical Specialists in the Planning Section or wherever their services are needed. The cyber specialists and their rules are this guide's practice.

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.