



Securing Tomorrow's Missions Today.



Your IR Plan Was Written for Rev. 2: A Fixed-Fee Incident Response Readiness Package

Security Incident Response & Forensic Analysis: realign the plan, write the playbooks, and test both against the reporting clock.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
Why Plans Stall on Paper	3
Why It Concentrates in Government	3
The Mandates and the Calendar	5
What the Readiness Package Does	7
Deliverables	9
What Follows, Conditionally	9
Evidence Assessors Can Use	10
How an Engagement Runs	11
What the Agency Provides	12
What Is Not Included	12
How Avalon Staffs It	13
Pricing and How to Buy	14
Illustration: The Rev. 2-to-Rev. 3 Readiness Gap	14
Playbook Backlog	15
The One-Hour Clock	16
What the Package Costs	17
Common Pitfalls	18
Conclusion and Next Step	18
Appendices	19
Appendix A: Glossary	19
Appendix B: Illustration Assumptions	19
Appendix C: References	20

Executive Summary

Most federal incident response plans were written once, approved, and filed. Many still follow the four-phase lifecycle of NIST SP 800-61 Rev. 2. Few have been exercised against a realistic scenario since they were signed, and fewer still have been tested against the clock that matters most in the first hour: the requirement to notify CISA within one hour of identifying an incident.

The guidance has moved. NIST SP 800-61 Rev. 3, final in April 2025, replaced the Rev. 2 lifecycle and organizes incident response around the six functions of the NIST Cybersecurity Framework 2.0, including Govern. OMB M-26-14 (May 2026) replaced M-21-31 with a risk-based logging model, which decides what an investigator will have to work with. CISA BOD 26-04 (June 2026) set risk-based remediation clocks, the shortest of them three days with forensic triage.

This paper is for the people who own that gap: CISOs and deputy CISOs who fund readiness, SOC leads who would run the response, ISSMs and ISSOs who need IR-2, IR-3 and IR-8 evidence in the authorization record, CIOs, and the CORs who buy the work. It describes Avalon Technology Services' Security Incident Response & Forensic Analysis service, which starts with one engagement:

- **A fixed-fee Incident Response Readiness Package.** A gap review of the existing plan against SP 800-61 Rev. 3 and CSF 2.0, a realigned plan, scenario playbooks, one facilitated tabletop with an after-action report and corrective-action register, and a walk-through of the reporting clocks. Unclassified, remote-first, business hours, typically 3 to 8 weeks, priced inside a \$35K to \$90K plan-and-tabletop band.
- **Conditional follow-ons.** A retainer, live incident response and forensic acquisition, quoted only when named certified responders, licensed tooling, an evidence-storage arrangement, insurance and a signed surge partner are in place for that engagement.

Section 9 works through an illustrative agency whose plan has 15 core elements: 3 are current, 7 need realignment to Rev. 3 and 5 are missing. 4 of 5 scenario playbooks need writing or realignment, and in a tabletop the team can produce 4 of the 8 pieces of information the one-hour notification needs. The fixed fee for that package is \$60K.

The service prepares and evidences. It does not assess its own work, grant an authorization, make breach determinations or report incidents on the agency's behalf. Those belong to the agency's assessor, its Authorizing Official, its counsel and privacy official, and the agency itself.

Why Plans Stall on Paper

An incident response plan can pass an annual policy review for years and still fail in the first hour of a real incident, because nobody has walked through it with the people who would use it.

What people say	What it usually means
"Our IR plan hasn't been exercised since it was written."	No IR-3 testing evidence, and no way to know which steps work
"Our SOC monitors, but nobody here does forensics."	Detection exists; investigation, evidence handling and scoping do not
"We reported it to CISA, but we couldn't answer their follow-up questions."	The notification was sent; the facts behind it were not ready
"The IG asked for the evidence and we had screenshots."	No evidence-preservation or chain-of-custody procedure
"Legal asked what data was accessed and we couldn't say."	Log sources and retention do not support the questions an investigation asks
"Who can approve isolating a mission system at 2 a.m.?"	No named incident commander with authority to approve containment

Why It Concentrates in Government

- **The plan answers to a policy cycle, not an adversary.** IR-8 asks for a plan, and annual reviews confirm it exists. Without an exercise, nobody tests whether its steps, contacts and authorities still work.
- **The SOC is a contract with a scope.** A contracted SOC monitors and escalates. Investigation, scoping and evidence handling often sit outside that scope, and the gap appears during the first real incident.
- **Decisions are spread across offices.** Containment belongs to the system owner and the incident commander, reporting to the CISO, breach analysis to counsel and the privacy official. A plan that does not name them leaves those calls to be negotiated mid-incident.

- **CISA's response bench is stretched.** CISA advises and coordinates, but the agency still owns its investigation, its evidence and its answers to follow-up questions.

The Mandates and the Calendar

Driver	What it requires	What it means for the plan
NIST SP 800-61 Rev. 3 (April 2025)	Incident response recommendations organized around CSF 2.0's six functions; Rev. 2's four-phase lifecycle is superseded	Plans written to Rev. 2 need realignment, starting with governance and roles
CISA Federal Incident Notification Guidelines	Report incidents to CISA within one hour of identification	The plan names who drafts, who approves and who submits, and where each fact comes from
DFARS 252.204-7012 (DoD contractor context)	Contractors report cyber incidents within 72 hours and preserve images for 90 days	DoD offices overseeing contractors need playbook steps that match the contractor's clock
OMB M-26-14 (May 2026)	Risk-based logging model; replaced M-21-31	Log sources and retention decide which questions an investigation can answer
CISA BOD 26-04 (Jun 10, 2026)	Risk-based remediation clocks from 3 days with forensic triage to the next upgrade; replaced BOD 22-01 and BOD 19-02	The shortest clock assumes the agency can triage forensically on demand
CISA BOD 26-02 (Feb 6, 2026)	End-of-support edge devices: inventory in 3 months, decommission in 12, replace in 18	Edge-device compromise belongs in the playbook set
CISA federal IR playbooks (2021, under EO 14028)	Standard incident and vulnerability response process for civilian agencies	The structure agency playbooks are measured against
OMB M-17-12	Breach preparedness and response for personally identifiable information	Breach determinations stay with counsel and the privacy official; the plan hands them facts

For DoD components, RMF, DoDI 8510.01 and eMASS remain in use under the Cybersecurity Risk Management Construct announced in September 2025, so IR testing evidence goes into the same record it does today. The CIRCIA reporting rule for critical infrastructure entities is expected but not in force as of this writing; it is aimed at critical infrastructure owners and operators, while federal agencies report under the CISA notification guidelines described above.

Three buying moments recur: fiscal year-end operations funds (July through September), a new CISO's first 90 days, and an authorization where the assessor asks for IR-3 testing evidence. A peer agency's incident or an inspector general finding can move any of them forward.

What the Readiness Package Does

The entry engagement answers four questions for one agency or bureau: what in the plan still fits Rev. 3, what the team would do in its likely scenarios, whether it can meet the reporting clock, and what to fix first.

Workstream	Activities
Gap review	Tag every element of the existing plan as current, needing realignment or missing against SP 800-61 Rev. 3 and the CSF 2.0 functions, from document review and interviews with the SOC lead, ISSM and system owners
Plan realignment	Rewrite the plan to the Rev. 3 structure: roles and authorities, a named incident commander, third-party responsibilities, escalation criteria, evidence preservation, reporting and recovery validation
Scenario playbooks	Step-by-step playbooks for the agency's likely scenarios: ransomware, business email compromise, credential theft, edge-device compromise and data exfiltration, aligned to the CISA federal playbooks
Tabletop exercise	One facilitated exercise built on one of the playbooks, with injects timed against the one-hour CISA notification (and the 72-hour DFARS clock where it applies)
After-action and corrective actions	An after-action report and a corrective-action register mapped to IR-2, IR-3, IR-4, IR-6 and IR-8, with owners and dates set by the agency

Deliverables

Deliverable	Format
Gap review of the current plan against Rev. 3 and CSF 2.0	Spreadsheet, one row per plan element, plus a short briefing
Realigned incident response plan	Editable document in the agency's template, plus PDF of record
Scenario playbooks	Editable documents, one per scenario
Tabletop package	Scenario injects, facilitator guide, participant materials
After-action report	PDF, written as IR-3 testing evidence
Corrective-action register	Spreadsheet or tracker export that can feed the agency's POA&M

What Follows, Conditionally

A retainer, live incident response and forensic acquisition are the other half of this service. They are quoted only when, for that engagement, named responders with incident handling and forensic certifications (such as GCIH or GCFA) are listed in the proposal, a licensed forensic suite is in hand, an evidence-storage arrangement and written chain-of-custody procedure exist, the coverage the solicitation requires is in place, and a surge partner is under a signed agreement. Any response commitment is business-hours remote initiation that the named responder can staff. None of this is committed by buying the readiness package.

Evidence Assessors Can Use

Control	Evidence the package produces
IR-1	Plan linked to the agency's IR policy; the -1 control in each family covers policy and procedures
IR-2	Role-based training content and the tabletop participant record
IR-3	Tabletop scenario, injects, participant list and after-action report
IR-4	Realigned handling procedures and scenario playbooks
IR-5, IR-6	Incident tracking fields and the notification walk-through: who drafts, approves and submits
IR-7	Named sources of assistance, including CISA and any contracted support
IR-8	The realigned plan, with roles, authorities and third-party responsibilities
AU-6, SI-4	Escalation criteria from monitoring to a declared incident; log sources an investigation needs

For DoD contractor contexts, the same work maps to NIST SP 800-171 requirements 3.6.1 through 3.6.3 (incident handling, reporting and testing). These are preparer artifacts. The agency's assessor draws assessment conclusions, and the Authorizing Official decides.

Accurate	Not accurate
Realigns the plan consistent with NIST SP 800-61 Rev. 3	Makes the agency compliant with the IR family
Produces implementation and testing evidence for IR controls	Satisfies the assessor or results in an ATO
Supports the agency's reporting obligations to CISA and OMB	Reports incidents on the agency's behalf
Characterizes tradecraft from the data examined (follow-on work)	Names the actor behind an intrusion

How an Engagement Runs

Phase	Typical duration	What happens
Kickoff and data call	Week 1	Sponsor alignment, current plan and playbooks, SSPs, prior incident and exercise records, contact lists
Gap review	Weeks 1–2	Document review, interviews, gap register by CSF 2.0 function
Plan and playbooks	Weeks 2–5	Realigned plan, scenario playbooks, agency review cycle
Tabletop	Weeks 5–7	Scenario design, injects, facilitation (half a day, remote or on-site by agreement)
After-action and closeout	Weeks 6–8	After-action report, corrective-action register, closeout briefing

Tabletop and plan work typically runs 3 to 8 weeks. The schedule starts when the documents and interviews are available, not at award.

What the Agency Provides

- A sponsor, usually the CISO or deputy, and a named incident commander who can speak for containment decisions in the tabletop.
- The current plan, playbooks, SSPs, network diagrams, asset inventory and records of prior incidents and exercises.
- Time from the SOC lead, ISSM or ISSO, system owners and a network engineer for interviews and the exercise.
- Counsel and the privacy official engaged for the reporting and breach portions, since those decisions are theirs.
- Review of drafts within the agreed revision cycle (two rounds are included).

What Is Not Included

Included	Separate work
Plan, playbooks, tabletop and corrective-action register	24x7 monitoring or managed SOC operation
Reporting-clock walk-through and draft notification content	Submitting reports to CISA or DoD, which the agency does
Corrective actions named and mapped to controls	Enterprise remediation or patching
Evidence-preservation procedure in the plan	Live forensic acquisition (conditional follow-on)
Facts for counsel and the privacy official	Breach determinations, notification decisions, legal advice
Characterization of tradecraft (follow-on work)	Attribution, ransom negotiation or payment advice
Unclassified environments	Classified systems and spillage handling

How Avalon Staffs It

Avalon takes one engagement at a time, works in unclassified environments only, and delivers during business hours. The readiness package is led by Avalon's founder with one named technical lead who has hands-on incident handling experience, hired or subcontracted and listed in the proposal. Avalon has no past federal engagements under this service, and it cites no certification, clearance or past engagement that is not current and verifiable.

Requirement	How it is handled
Technical lead	Named personnel whose certifications and investigation level match the agency's requirements, listed in the proposal
Responders for any follow-on	Named, certified responders (such as GCIH or GCFA) as a condition of any retainer or live response
Forensic tooling and evidence storage	A licensed forensic suite, evidence storage and a written chain-of-custody procedure as conditions of any acquisition work
Response commitments	Business-hours remote initiation only, at a level the named responder can staff; no 24x7 commitment
DoD work roles and civilian access	DoD 8140 qualification or the Public Trust tier the agency requires, as a condition of the engagement
Insurance and contract vehicles	Any coverage the solicitation requires is a condition of award; Avalon does not hold a GSA Schedule or a governmentwide contract today

Pricing and How to Buy

Engagement	Market-norm range	Pricing basis
Tabletop exercise with after-action report	\$15K–\$50K	Firm fixed price
IR plan and playbook development or overhaul	\$20K–\$75K	Firm fixed price
Avalon entry: plan and tabletop bundle	\$35K–\$90K	Firm fixed price
Annual retainer (conditional follow-on)	\$50K–\$250K	Fixed fee plus prepaid hours
Contained single-system response (conditional)	\$25K–\$75K	Time and materials with a not-to-exceed
Forensic deep-dive per system (conditional)	\$8K–\$20K	Per-system unit

Senior incident response labor in a federal context runs roughly \$175 to \$325 an hour. The readiness package fits well under the \$350,000 simplified acquisition threshold, so it can be bought open-market with one-year operations funds, or as a subcontract under a prime's security task order. Purchases between the \$15,000 micro-purchase threshold and the threshold are generally set aside for small business when two or more capable small businesses are expected to compete. Avalon does not hold a GSA Schedule or a governmentwide contract today.

Enterprise-scale response is not offered by Avalon as sole performer.

Illustration: The Rev. 2-to-Rev. 3 Readiness Gap

The figures below are a planning illustration for one representative small civilian agency, not a quote and not a result from any engagement. Every plan element, status and count is an assumption.

The gap review tags each element of the existing plan as **current**, **needs realignment** (present but written to the Rev. 2 lifecycle or out of date) or **missing**, grouped by CSF 2.0 function.

CSF 2.0 function	Elements	Current	Realign	Missing	Gaps
Govern	3	1	1	1	2
Identify	2	0	1	1	2
Protect	2	0	1	1	2
Detect	2	0	2	0	2
Respond	4	1	2	1	3
Recover	2	1	0	1	1
Total	15	3	7	5	12

12 of 15 elements need work. The Govern and Respond functions carry the decisions that matter most in the first hour: no third-party responsibilities for the contracted SOC or cloud providers, a notification step that names nobody to approve it, and no evidence-preservation procedure. Recover has one gap, and it is the one that lets an adversary back in: no clean-state check before restored systems return to service.

Playbook Backlog

Scenario playbook	Status
Ransomware	Current
Business email compromise	Missing
Credential theft and account takeover	Missing
Edge-device compromise	Missing
Data exfiltration	Needs realignment

4 of 5 playbooks need writing or realignment. Edge-device compromise is the obvious gap, given BOD 26-02 and the forensic triage clock in BOD 26-04.

The One-Hour Clock

The tabletop times the team against the one-hour notification. The last exercise was 30 months ago. The assumed result:

Information needed	Within the hour?	Where it would come from
Agency point of contact and reporting official	Yes	Contact tree
Time of detection and time of identification	Yes	SIEM alert and ticket
Affected systems and their criticality	No	Asset inventory (not reconciled)
Functional impact on the mission	No	System owner (not on the call tree)
Information impact (what data may be involved)	No	Data inventory and logs
Attack vector, if known	Yes	EDR console
Indicators observed	Yes	EDR and SIEM
Actions taken so far	No	No running incident log

The team can produce 4 of the 8 items inside the hour. The four it cannot are the ones CISA's follow-up questions turn on: which systems, what mission impact, what information, and what has been done so far. Each becomes a corrective action with an owner.

The corrective-action register for this agency holds 13 items: 4 against IR-8 (plan, roles, third parties), 4 against IR-4 (handling, evidence, recovery), 2 against IR-6 (reporting), and one each against IR-2, IR-3 and AU-6.

What the Package Costs

Scenario	Hours	Rate-band range	Fixed fee	Plan line	Tabletop line
Narrow (3 playbooks)	224	\$39.2K–\$72.8K	\$56K	\$36K	\$20K
Base (4 playbooks, one tabletop)	240	\$42K–\$78K	\$60K	\$40K	\$20K
Broad (6 playbooks, larger plan)	292	\$51.1K–\$94.9K	\$73K	\$54K	\$19K

Hours: intake and gap review 24, plan realignment 60 (80 in the broad case), 16 per playbook, tabletop design 40, facilitation 8, after-action 24, project management 20. Rates \$175, \$250 and \$325 an hour; fixed fee at \$250.

In the base case, 240 hours at mid-band rates price at \$60K, inside the \$35K to \$90K entry band, with a plan line of \$40K (inside the \$20K to \$75K plan band) and a tabletop line of \$20K (inside the \$15K to \$50K tabletop band). Three playbooks bring it to \$56K. The broad case, six playbooks and a larger plan, prices at \$73K at mid-band, but at the top of the rate band it reaches \$94.9K, above the bundle band; at that size it is better quoted as separate plan and tabletop line items inside their own bands. A second tabletop is priced the same way, as its own line item.

Common Pitfalls

Pitfall	How to avoid it
A plan rewritten without an exercise	Bundle the tabletop with the plan so the plan is tested before it is filed
"While you're in here" remediation	A boundary clause: corrective actions are named and handed to the agency, and remediation is separate work
Report-revision loops	A fixed number of review rounds, stated in the statement of work
Retainer pricing that undercuts the tabletop	Price the retainer at no less than the standalone tabletop plus its hours
Investigative advice before a contract	No incident details over unencrypted email and no investigative direction until a contract exists
Touching original evidence	In any follow-on, work from verified copies and document chain of custody on every acquisition

Conclusion and Next Step

An incident response plan earns its value in the first hour of a real incident, and most federal plans have never been tested against that hour. A realigned plan, playbooks for the likely scenarios and one honest tabletop against the reporting clock turn a filed document into a tested capability, and give the ISSM the IR-3 evidence the authorization record asks for.

The natural first step is the fixed-fee Incident Response Readiness Package: one agency or bureau, a defined scope well under the simplified acquisition threshold, a gap review, a realigned plan, scenario playbooks, a tabletop and a corrective-action register. To discuss a readiness package, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

After-action report

The written record of an exercise or incident: what happened, what worked, what did not, and the corrective actions.

Chain of custody

The documented record of who collected, held and transferred each piece of evidence, with hashes recorded at acquisition.

CSF 2.0

NIST Cybersecurity Framework 2.0, with six functions: Govern, Identify, Protect, Detect, Respond and Recover.

Incident commander

The agency official with authority to approve containment actions such as isolating a mission system.

Playbook

A scenario-specific, step-by-step response procedure that sits under the incident response plan.

Tabletop exercise

A facilitated, discussion-based walk-through of a scenario, used to test a plan without touching production systems.

Corrective-action register

A tracked list of fixes from an exercise or incident, each with an owner, a date and a mapped control.

Appendix B: Illustration Assumptions

All values are planning assumptions for one representative small civilian agency. None is drawn from a specific agency or a completed engagement.

Assumption	Value	Basis
Plan elements reviewed	15 across the six CSF 2.0 functions	Planning assumption
Status mix	3 current, 7 needs realignment, 5 missing	Planning assumption
Playbooks	5 scenarios; 4 to write or realign	Planning assumption
Last exercise	30 months before the engagement	Planning assumption
Notification information	4 of 8 items producible within one hour	Planning assumption
Hours	240 in the base case	Planning build for this paper
Rates	\$175–\$325 an hour; fee at \$250	KB market-norm band
Price check	Base fee \$60K	Inside the \$35K–\$90K entry band

Appendix C: References

1. **Office of Management and Budget**, *M-26-14, Ensuring Effective and Efficient Agency Logging and Network Visibility to Defend Against Evolving Cyber Threats*, May 2026
<https://www.whitehouse.gov/wp-content/uploads/2026/05/M-26-14-Ensuring-Effective-and-Efficient-Agency-Logging-and-Network-Visibility-to-Defend-Against-Evolving-Cyber-Threats.pdf>
2. **National Institute of Standards and Technology**, *SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management*, April 2025
<https://csrc.nist.gov/pubs/sp/800/61/r3/final>
3. **National Institute of Standards and Technology**, *SP 800-86, Guide to Integrating Forensic Techniques into Incident Response*
<https://csrc.nist.gov/pubs/sp/800/86/final>

4. **National Institute of Standards and Technology**, *SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations*
<https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>
5. **Cybersecurity and Infrastructure Security Agency**, *Federal Incident Notification Guidelines*
<https://www.cisa.gov/federal-incident-notification-guidelines>
6. **Cybersecurity and Infrastructure Security Agency**, *Federal Government Cybersecurity Incident and Vulnerability Response Playbooks*
<https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks>
7. **Cybersecurity and Infrastructure Security Agency**, *Cybersecurity Directives*
<https://www.cisa.gov/news-events/directives>
8. **Defense Federal Acquisition Regulation Supplement**, *252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting*
<https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting>
9. **Tenable**, *CISA BOD 26-04 FAQ: Vulnerability Remediation Impact, June 11, 2026*
<https://www.tenable.com/blog/cisa-bod-26-04-faq-vulnerability-remediation-impact>
10. **Centre Law & Consulting**, *Inflation Updates to FAR Thresholds: What Changed on October 1, 2025*
<https://centrelawgroup.com/blog/inflation-updates-to-far-thresholds-what-changed-on-october-1-2025/>