Written Comments

Submitted by the

Center for Internet Security

November 3, 2023

Regarding the

Exposure Draft of the
NAIC's Cybersecurity Event Response Plan (CERP)

Issued on

Wednesday, October 4, 2023

By the

Cybersecurity (H) Working Group

National Association of Insurance Commissioners

Introduction

Established in 2000 as an independent nonprofit organization, the Center for Internet Security's mission is to make the connected world a safer place by using open, collaborative deliberation processes to define, share, and sustain security best practices against cyber threats. These best practices represent the consensus opinion of experts from across the global security community and are freely available to all enterprises. CIS has over 20 years of success in developing, sharing, and sustaining security best practices, powered by a successful nonprofit business model. For example, CIS was instrumental in establishing the first public guidelines for security hardening of commercial IT systems (now known as CIS Benchmarks) when there was little online security leadership – and CIS is now the world's largest independent source of security configuration hardening.[1]

CIS operates both the Multi-State Information Sharing and Analysis Center ("MS-ISAC") and the Elections Infrastructure ISAC ("EI-ISAC"). Currently, these two ISACs provide cyber threat-sharing information and some cybersecurity defensive tools to all 56 states and territories and over 16,000 tribal and local government organizations.[2] Both ISACs work to improve the overall cybersecurity posture of the nation's SLTT governments through coordination, collaboration, cooperation, relevant and timely communication, and cybersecurity capabilities.

In addition, CIS is the home of the CIS Critical Security Controls,[3] the set of internationally-recognized, prescriptive, prioritized operational security practices that form the foundation of essential cyber hygiene--network defense that is demonstrated to prevent 80-90% of all known pervasive and dangerous cyberattacks. By design, the CIS Controls help implement the goals of the NIST framework by providing a roadmap for network operators to improve cybersecurity by identifying specific actions to be done in priority order based on the current state of the global cyber threat. What results is the clearest, most definitive blueprint of how to protect an organiza-

---

[1] For more information about the Center for Internet Security, please see: www.cisecurity.org

[2] For more information about the MS- and EI-ISACs, please see: https://www.cisecurity.org/ms-isac and https://www.cisecurity.org/ei-isac, respectively.

[3] For more information about the CIS Critical Security Controls, please see: https://www.cisecurity.org/controls

tion from cyberattacks. While the NIST Cybersecurity Framework ("NIST CSF") is the *what*--NIST defines the categories of cybersecurity and an organizational view of security risk management—the Controls are the *how*--the prioritized technical pathway to achieve the NIST goals. Moreover, the CIS Controls are specifically referenced in the NIST CSF as one of the tools to implement an effective cybersecurity program.[4]

CIS's ability to develop useful, real-world security practices like the CIS Controls is driven by our large-scale activity to gather feedback from worldwide users of our guidance and our nationwide, 24x7 mission operating the two ISACs (supporting all 56 states and territories and over 16,000 local and tribal government organizations).

Recommendations

"The primary goal of incident response is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm. Without understanding the full scope of an incident, how it happened, and what can be done to prevent it from happening again, defenders will just be in a perpetual "whack-a-mole" pattern."[5]

CIS commends the National Association of Insurance Commissions for seeking concrete ways to assist state departments of insurance in responding to cybersecurity incidents at a regulated insurance entity. We respectfully recommend for your consideration four cyber incident response documents:

(1) the Incident Response Commander Flowchart[6];

(2) the Incident Handling Commander Flowchart[7];

(3) the Incident Response Management Policy Template for CIS Control 17[8]; and

---

[4] NIST Cybersecurity Framework, Appendix A, page 20, and throughout the Framework Core (referred to as "CCS CSC" - Council on Cyber Security (the predecessor organization to CIS for managing the Critical Security Controls): https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[5] Center for Internet Security, Incident Response Management Policy Template for CIS Control 17; page 4: https://www.cisecurity.org/insights/white-papers/incident-response-policy-template-for-cis-control-17

[6] Attached to the transmittal of this comment at Appendix 1.

[7] Attached to the transmittal of this comment at Appendix 2.

[8] Attached to the transmittal of this comment at Appendix 3 and available at this link: https://www.cisecurity.org/insights/white-papers/incident-response-policy-template-for-cis-control-17

(4) the CIS Cyber Incident Checklist, intended for executives[9].

The first two documents resulted from efforts by the MS-ISAC's Business Resiliency Workbench Working Group. They are the current community-driven recommendations to help entities operationalize their IR plans. These were developed as a result of several key factors:

- Feedback from a poll question during an incident response webinar series where 97% of participants for that particular session said they would use CIRT for incident response *planning* if it was offered
- Individual outreach from SLTTs requesting assistance with their incident response plans (IRPs)
- Growing support within the SLTTs to assist others in identifying responsibilities/roles and helping to develop IRPs (i.e., crowdsourcing), and
- Identification of what seemed to be a trend of SLTTs developing IRPs that were not customized for operations. For example:
    - IRPs would be large, lengthy, complicated documents that would be too cumbersome to refer to at the time of action
    - IRP structure was lacking or inconsistent
    - Many templates were grabbed from the Internet and not customized to the organization
    - The IRPs often lacked clear roles and responsibilities with defined processes and workflows

The Business Resiliency Working Group that helped develop these two flowcharts currently consists of 34 members across CIS and our SLTT community including 5 critical infrastructure members, 2 states, 2 elections, 12 local governments (counties and below), 4 K-12, and 1 tribal member.

The third document, the *Incident Response Management Policy Template for CIS Control 17*, was developed as a support document for the CIS Critical Security Controls, the set of internationally-recognized, prescriptive, prioritized operational security practices that form the foundation of essential cyber hygiene--network defense that is demonstrated to prevent 80-90% of all

[9] Attached to the transmittal of this comment at Appendix 4.

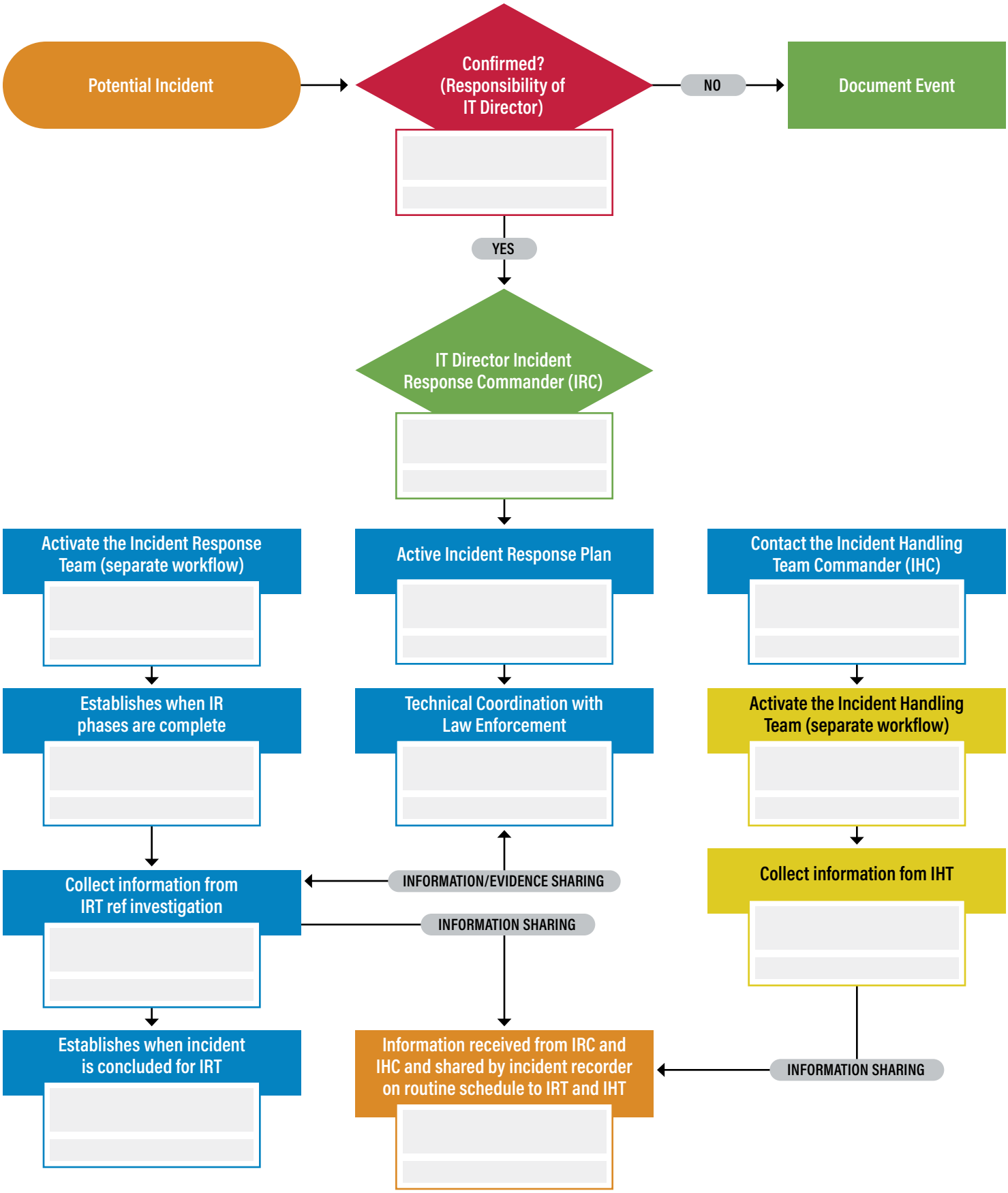
known pervasive and dangerous cyberattacks. The CIS Controls recommend multiple information security policies that an enterprise should have in place. This *Incident Response Policy* is meant as a starting point for organizations needing to draft their own policies and provides specific, high-level steps that should be part of any comprehensive incident response plan. Enterprises are encouraged to use this policy template in whole or in part. Obviously, there are multiple decision points and areas that must be tailored to your enterprise.

The fourth document is a cyber incident checklist designed for executives of both public and private sector organizations. The checklist identifies specific tasks that senior officials should focus on in three areas during a cyber incident: (1) establish reliable facts and a way to stay informed; (2) mobilize a response; and (3) communicate what you know.

We hope that these documents help inform the CERP's ability to support state departments of insurance in their response to notifications of cybersecurity events at regulated insurance entities. Please feel free to contact us if we can answer any questions that you might have or assist you in this important aspect of defending our nation.

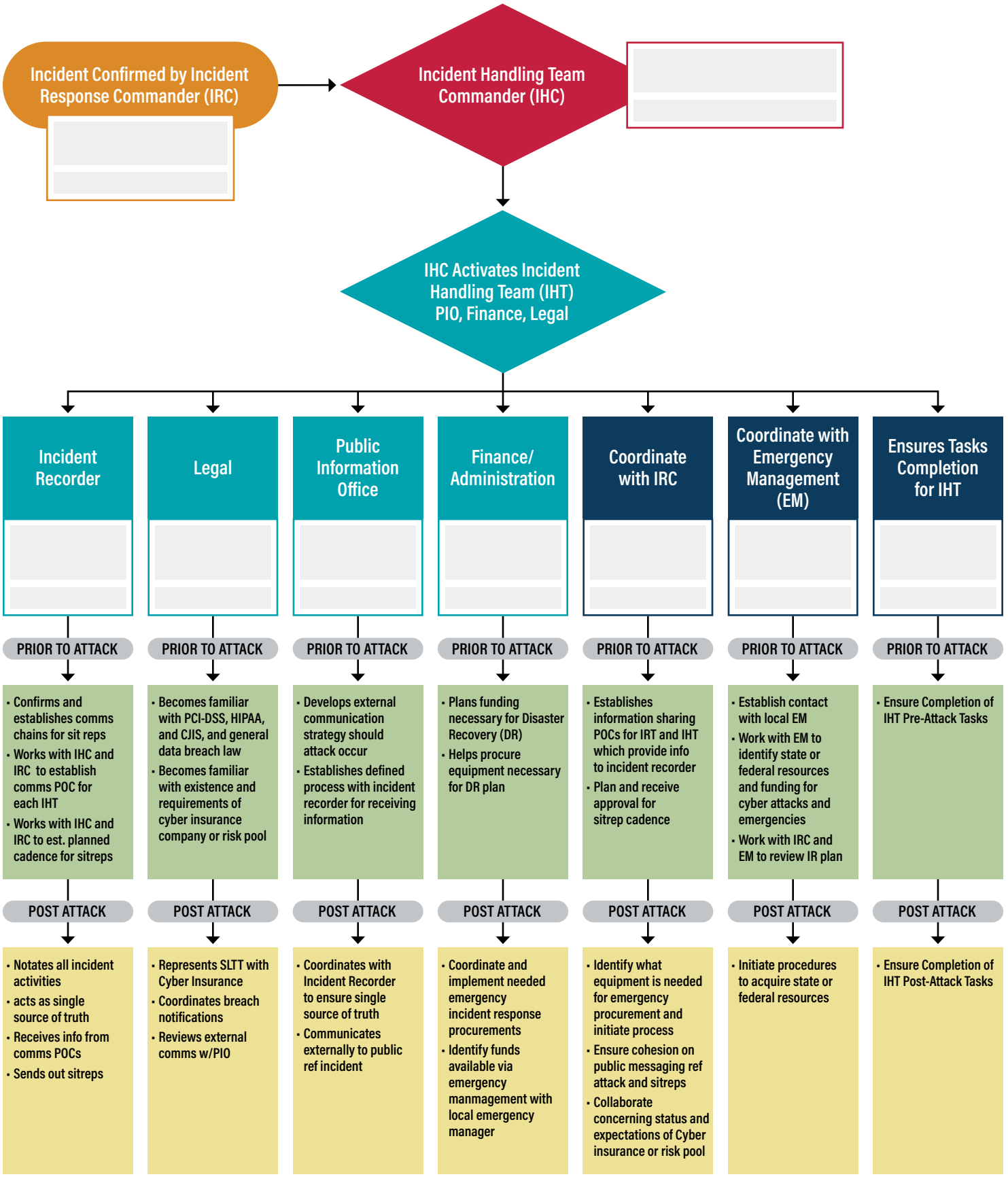
Incident Response Commander Flowchart

MS-ISAC®
Multi-State Information Sharing & Analysis Center®



Incident Handling Commander Flowchart

MS-ISAC®
Multi-State Information Sharing & Analysis Center®



Incident Response Policy Template

Critical Security Controls

March 2023

Contents

Acknowledgments

The Center for Internet Security® (CIS®) would like to thank the many security experts who volunteer their time and talent to support the CIS Critical Security Controls® (CIS Controls®) and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

Editors:

Joshua M Franklin, CIS

Contributors:

Tony Krzyzewski, SAM for Compliance Ltd
Staffan Huslid, Truesec
Diego Bolatti, Information Systems Engineer, Universidad Tecnológica Nacional (Argentina)
Bryan Chou, CISSP, GSEC, GCED, GCIH
Bryan Ferguson
Gavin Willbond, SSS - IT Security Specialists
Ken Muir
Keala Asato
Jon Matthies
Chris Davis
Robin Regnier, CIS
Valecia Stocchetti, CIS

Introduction

A comprehensive cybersecurity program includes protections, detections, response, and recovery capabilities. Often, the final two get overlooked in immature enterprises, or the response technique to compromised systems is just to re-image them to original state, and move on. The primary goal of incident response is to identify threats on the enterprise, respond to them before they can spread, and remediate them before they can cause harm. Without understanding the full scope of an incident, how it happened, and what can be done to prevent it from happening again, defenders will just be in a perpetual "whack-a-mole" pattern.

We cannot expect our protections to be effective 100% of the time. When an incident occurs, if an enterprise does not have a documented plan—even with good people—it is almost impossible to know the right investigative procedures, reporting, data collection, management responsibility, legal protocols, and communications strategy that will allow the enterprise to successfully understand, manage, and recover.

Along with detection, containment, and eradication, communication to stakeholders is key. If we are to reduce the probability of material impact due to a cyber event, the enterprise's leadership must know what potential impact there could be, so that they can help prioritize remediation or restoration decisions that best support the enterprise. These business decisions could be based on regulatory compliance, disclosure rules, service-level agreements with partners or customers, revenue, or mission impacts.

Dwell time from when an attack happens to when it is identified can be days, weeks, or months. The longer the attacker is in the enterprise's infrastructure, the more embedded they become and they will develop more ways to maintain persistent access for when they are eventually discovered. With the rise of ransomware, which is a stable moneymaker for attackers, this dwell time is critical, especially with modern tactics of stealing data before encrypting it for ransom.

Purpose

The CIS Critical Security Controls® (CIS Controls®) recommend multiple information security policies that an enterprise should have in place. This *Incident Response Policy* is meant as a "jumping off point" for organizations needing to draft their own policies, and provides specific, high-level steps that should be part of any comprehensive incident response plan. Enterprises are encouraged to use this policy template in whole or in part. With that said, there are multiple decision points and areas that must be tailored to your enterprise.

Events vs Incidents

There are many ways to define an incident. The authors of this document consider the following factors when defining an incident:

- An event or situation, either intentional or unintentional, internal to the enterprise or external,
- Caused by an individual, enterprise, nation state, or natural event that,
- Impacts an enterprise's ability to accomplish its mission (critically or otherwise), and
- This event may or may not lead to loss of data.

Examples of deliberate hacking incidents include attacks against Supermarket Chain Coop's and those affected by the SolarWinds Attacks. Incidents aren't always hacking-oriented as was the case with a French data center that was affected by fires, meaning natural disasters can also trigger the incident response plan. It can sometimes be difficult to interpret something as an *event* or an *incident*. NIST defines an *incident* as a "cybersecurity event that has been determined to have an impact on the organization prompting the need for response and recovery."[1] Some view an *event* as any occurrence that can be observed, verified, and documented, whereas an *incident* is one or more related events that negatively affect the company

[1] https://csrc.nist.gov/glossary/term/Cybersecurity_Incident

and/or impact its security posture. Sometimes one business unit within an enterprise will interpret an action as an event whereas another business unit will define it as an incident. This distinction matters, as an incident will trigger different enterprise responses, such as activating the incident response plan. Having clearly established definitions of events versus incident can be very beneficial for this reason. For example, an enterprise may determine that anytime leadership is actively involved in an event, it will be classified as an incident. Ultimately, this is a judgement call. Note that events can become incidents as more information is gathered.

Scope

This policy template is meant to supplement the CIS Controls v8. The policy statements included within this document can be used by all CIS Implementation Groups (IGs), but are geared towards Safeguards in Implementation Group 1 (IG1). Additional Safeguards from IG2 are included within this policy template, since they are commonly included as requirements from cyber insurance providers. These Safeguards are 17.4, 17.5, and 17.6. A mapping for Safeguards to the CIS Controls can be found in Appendix D. For more information on the CIS Implementation Groups, see Appendix C. Additionally, a glossary in Appendix B is provided for guidance on terminology used throughout the document. Future versions of this template may expand the scope to both Implementation Group 2 (IG2) Safeguards. IG2 and IG3 enterprises may feel the need to add sections that go beyond IG1, and are welcome to do so. Depending on an enterprise's sector or mission, other policy statements may also need to be added or removed. This is encouraged as this policy needs to be molded and fit to the enterprise's needs.

Incident Response Plan Lifecycle

This *Incident Response Policy Template* is divided into multiple sections based on usage patterns of assets within an enterprise. There are many ways to organize the incident response process. *The NIST Cybersecurity Framework (CSF)* provides one, as does *NIST 800-61 Revision 2: Computer Security Incident Handling Guide*. The lifecycle presented below in Figure 1 is an abstracted way to view the incident response process and house the policy statements provided by this document in an organized manner. High-level "steps" of the incident responses process are presented, followed by a detailed description of what each step entails.

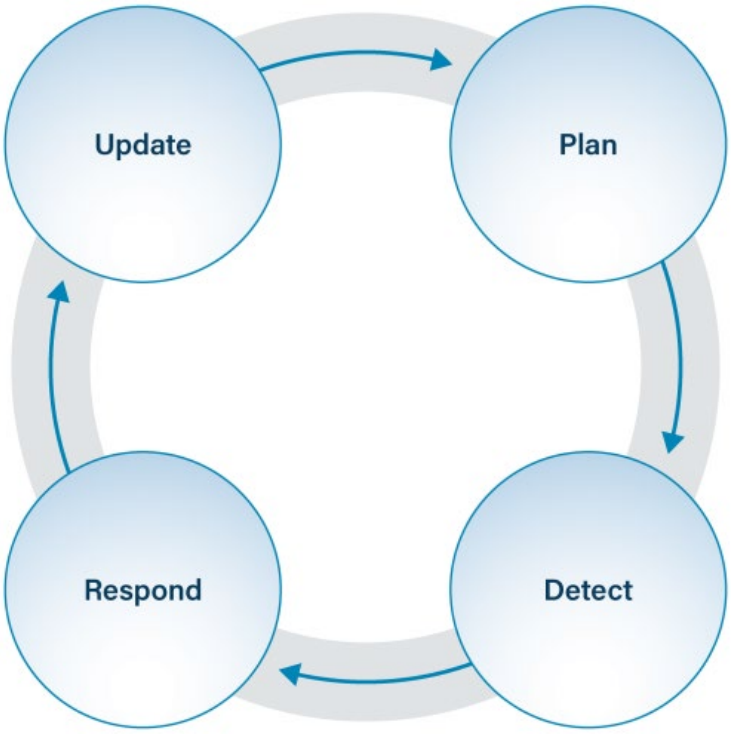


Figure 1. Incident Response Process

- **Plan** – Develop documentation for all procedures necessary to handle an incident.
- **Detect** – Monitor enterprise assets and analyze intelligence to understand if an incident has occurred.
- **Respond** – Activate the incident response plan to deal with an incident.
- **Update** – Understand which portions of the incident response plan have been effective or not, and update the plan accordingly.

Plan

When an incident occurs, the first step is to consult the incident response plan for the next steps that the enterprise should take. The plan should remain available in case enterprise systems are no longer functioning as intended; common methods include storing the plan on an external system or keeping a paper copy on hand. An incident will be a stressful time and this plan should provide step-by-step instructions that prevents guesswork during the heat of the moment. There are variety of incident response plans available online that enterprises can consult when writing their own plan. Plans will vary from enterprise to enterprise, but the level of detail will often be dictated by the maturity of the cybersecurity program. One of the most common aspects of an incident response plan is to name specific individuals to perform defined functions during this process. There will likely need to be someone who is responsible for the entire process, often the incident manager. Any

external support from third parties should also be named, which often includes contractors or technical organizations offering support. Detailed contact information should be provided for all individuals named in the plan. Once written, this plan will change over time as experience is gained, and the process gradually iterates to be in sync with the needs of the enterprise. Testing the plan via tabletop exercises is a great way to gain familiarity with the plan.

While larger enterprises may place procedures for responding to a natural disaster within a business continuity plan, smaller enterprises may place these policies within the incident response plan. Either approach is acceptable, and enterprises are encouraged to seek out how this is typically done in similar enterprises in their localities. Regulatory requirements may specifically note where these policies and procedures belong.

There is a need for a defined process for a user to report any identified event, or potential event. This process should be documented to facilitate clarity and ease of implementation. This is a separate plan or process from the Incident Response Plan. Users should be taught this process during the mandatory training for security awareness, therefore it must be easy to implement. The information should also be placed on internal intranet places and other logical places that would make the information readily available and accessible to all users.

Detect

Detecting if an incident occurred is difficult. Especially if the attack was subtle from advanced actors. To combat this, enterprises typically leverage a variety of methods to identify incidents such as data, anti-malware, and security awareness training. Data will often take the form of logs that must be analyzed. These logs may contain information to help you understand if an incident has occurred. Anti-malware tools such as endpoint detection and response (EDR) are tailor made for detecting these types of attacks. Finally, employees should be regularly trained on how to spot and report incidents. This means that IT must monitor employee reports of computer incidents and actively investigate such reports.

Respond

Once an incident has been reported or detected, IT, or the business units charged with security, must activate the incident response plan as developed in the planning phase. This response also begins the recovery process. The response team will often be composed of internal and external users all working together to carry out the incident response plan. It's common for smaller enterprises to contact any contractors helping to manage its IT infrastructure or any state/federal government entities offering free or low-cost services. Ultimately, the individual specified in the incident response plan as the incident manager is charged with ensuring the incident has been properly managed and is following established standard operating procedures (SOPs). It's best practice for the incident manager to be an individual trained in incident response with excellent communication skills, the capacity to prioritize the incident. This individual must have the authority to communicate business impacts with external organizations such as lawyers, regulators, cyber insurance companies, local cyber incident response teams (CIRT) and potentially law enforcement. Generally, this is not a senior executive; but this is not always practical with smaller entities. External incident response expertise may be required. This individual will also be responsible for making the determination that the incident has come to a conclusion.

Update

The update phase of this lifecycle ensures that the incident response plan and process is gradually improving from the experiences of recent incidents, tabletop exercises, and scheduled regular review. Lessons learned from recent incidents should be discussed with the individuals involved in the incident response process. Appropriate changes to the incident response plan based on recent incidents should be made, alongside the standard operating procedures. Where applicable, communicate and train staff on changes to the IR plan. During the incident response process, it's common for data to be collected and used to help guide actions of all involved. These collected data artifacts should be archived or deleted in a manner consistent with the *Data Management Policy* and documented it in the custodial chain of evidence if appropriate.

Incident Response Policy Template

Purpose

Incident response includes planning for and actively managing incidents that can prevent an enterprise from leveraging its assets to meet its goals. Most commonly this takes the form of unauthorized access into a computer system, physical security intrusions, or if a natural disaster occurs. The *Incident Response Policy* provides the processes and procedures for ensuring incidents are properly handled with as little impact to the enterprise as possible, and to begin the recovery plan. This policy applies to all departments and all assets connected to the enterprise network.

Responsibility

- The IT business unit is responsible for managing all incident response functions.
    - While all IT staff are required to follow the written incident response plan, real world deviations are expected and must be handled gracefully. Third-party organizations involved in the incident response process must be managed by the incident manager.
- Users are responsible for reporting incidents that they are aware of to the appropriate business unit or personnel as specified in the incident reporting process. Users are responsible for attending training for recognizing and reporting incidents within the enterprise.

Policy

Plan

1. IT must develop and maintain a written incident response plan.
    a. This process must be documented and approved.
    b. This plan must include a process for responding to incidents.
    c. At a minimum, the incident response process must be reviewed on an annual basis or following significant changes within the enterprise.
        a. This review may also occur following an incident or tabletop exercise.
    d. An incident manager and backup incident manager must be specifically identified by name within the plan.
        a. If an external party is the incident manager, then one internal individual must be specified to oversee the response process.
        b. Contact information must be recorded in the incident response plan.
    e. Any parties that need to be made aware of a security incident must be documented.
    f. The plan must address any regulatory or other compliance requirements.
    g. The plan must address communications.
2. IT must develop and maintain a written process for users to report incidents.
    a. This process must include approved methods for reporting incidents including:
        a. Primary and secondary methods for reporting.
        b. Specific recipients to receive incident reports.
        c. Any minimum information needed.
        d. Timeframes for reporting incidents.
    b. At a minimum, the incident reporting process must be reviewed on an annual basis or following significant changes within the enterprise.

Detect

There are no IG1 safeguards that support this portion of the incident response process.

Respond

There are no IG1 safeguards that support this portion of the incident response process.

Update

1. At a minimum, the incident response and reporting processes must be reviewed on an annual basis or following significant changes within the enterprise.

Revision History

Each time this document is updated, this table should be updated.

Version	Revision Date	Revision Description	Name

Appendix A: Acronyms and Abbreviations

CIS	Center for Internet Security
CIS Controls	Center for Internet Security Critical Security Controls
CIRT	Cyber Incident Response Team
COTS	Commercial-off-the-shelf
CSF	Cybersecurity Framework
EDR	Endpoint Detection and Response
IG	Implementation Group
IR	Incident Response
ISAC	Information Sharing and Analysis Center
IT	Information Technology
OSINT	Open-source intelligence
SOP	Standard Operating Procedure

Appendix B: Glossary

Asset	Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards). Source: Asset(s) - Glossary | CSRC (nist.gov)
Cloud environment	A virtualized environment that provides convenient, on-demand network access to a shared pool of configurable resources such as network, computing, storage, applications, and services. There are five essential characteristics to a cloud environment: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Some services offered through cloud environments include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).
Enterprise assets	Assets with the potential to store or process data. For the purpose of this document, enterprise assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers in virtual, cloud-based, and physical environments. Source: CIS Controls v8
Network devices	Electronic devices required for communication and interaction between devices on a computer network. Network devices include wireless access points, firewalls, physical/virtual gateways, routers, and switches. These devices consist of physical hardware as well as virtual and cloud-based devices. For the purpose of this document, network devices are a subset of enterprise assets. Source: CIS Controls v8
Physical environment	Physical hardware parts that make up a network, including cables and routers. The hardware is required for communication and interaction between devices on a network. Source: CIS Controls v8
Portable end-user devices	Transportable, end-user devices that have the capability to wirelessly connect to a network. For the purpose of this document, portable end-user devices can include laptops and mobile devices such as smartphones and tablets, all of which are a subset of enterprise assets. Source: CIS Controls v8
User	Employees (both on-site and remote), third-party vendors, contractors, service providers, consultants, or any other user that operates an enterprise asset. Source: CIS

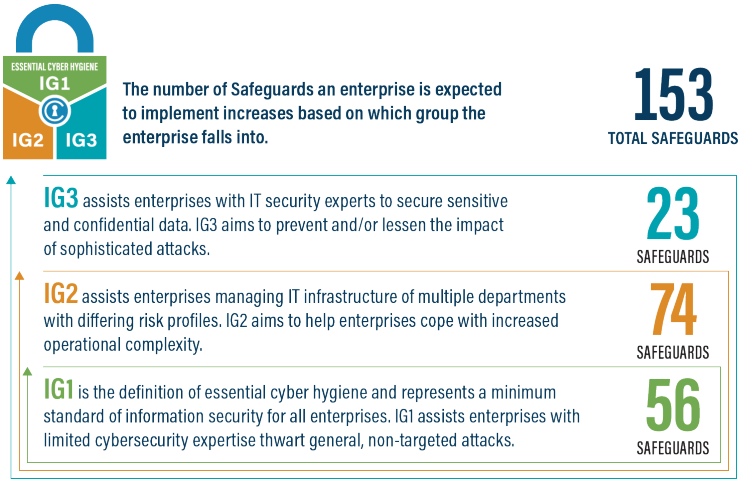
Virtual environment	Simulates hardware to allow a software environment to run without the need to use a lot of actual hardware. Virtualized environments are used to make a small number of resources act as many with plenty of processing, memory, storage, and network capacity. Virtualization is a fundamental technology that allows cloud computing to work. Source: CIS Controls v8

Appendix C: Implementation Groups

As a part of our most recent version of the CIS Controls, v8, we created Implementation Groups (IGs) to provide granularity and some explicit structure to the different realities faced by enterprises of varied sizes.

IG1

An IG1 enterprise is small- to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information. Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.



IG2

An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise information, and they can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

IG3

An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

If you would like to know more about the Implementation Groups and how they pertain to enterprises of all sizes, there are many resources that explore the Implementation Groups and the CIS Controls in general on our website at https://www.cisecurity.org/controls/cis-controls-list/.

Appendix D: CIS Safeguards Mapping

CIS Controls & Safeguards Covered by this Policy

This policy helps to bolster IG1 Safeguards in CIS Control 17: *Incident Response Management*. Table 1 shows which IG1 Safeguards are covered by this policy as written.

Table 1 - Safeguards covered by IG1

CIS Control	Policy Statement	CIS Safeguard Title	CIS Safeguard Description
17.1	Plan 1d	Designate Personnel to Manage Incident Handling	Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
17.2	Plan 1db	Establish and Maintain Contact Information for Reporting Security Incidents	Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.
17.3	Plan 2	Establish and Maintain an Enterprise Process for Reporting Incidents	Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
17.4	Plan 1	Establish and Maintain an Incident Response Process	Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant enterprise changes occur that could impact this Safeguard.
17.5	Plan 1de	Assign Key Roles and Responsibilities	Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, human resources, incident responders, and analysts, as applicable. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

CIS Control	Policy Statement	CIS Safeguard Title	CIS Safeguard Description
17.6	Plan 1g	Define Mechanisms for Communicating During Incident Response	Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant enterprise changes occur that could impact this Safeguard.

Cyber Incident Checklist

Center for Internet Security®

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Elections Infrastructure ISAC®

1

Establish Reliable Facts and a Way to Stay Informed

- ◯ **Who** is reporting the problem? How did they become aware?
- ◯ **What** do we know so far about what happened?
  - What networks/systems are affected?
  - What data/information was compromised (e.g., stolen, deleted, altered)?
- ◯ **When** did the breach occur?
  - When did we find out about it?
  - When did we begin to do some thing about it?
  - When will we know the full scope of the problem?
  - When do we estimate that the problem will be remediated?
- ◯ **Where** did the breach occur (what office, activity, locale, etc.)?
- ◯ **How** much do we know, with certainty, about how the breach occurred? The source of the attack?
- ◯ **How** will we stay informed of efforts to remediate the breach and restore normal service?

2

Mobilize a Response

- ◯ Who has the lead in directing operational response efforts? What role will your office play?
- ◯ Has the MS- or EI-ISAC been notified (+1 866.787.4722)?
- ◯ Who else should be notified at this point (e.g., citizens, business and industry, other state, local, federal officials)?
- ◯ Has law enforcement been notified?
- ◯ What expertise is on hand to work the problem? What additional help do you need? Who will provide it?
- ◯ What measures are needed to secure the networks/systems from further exploitation?
- ◯ What additional steps are needed to secure data holdings?
- ◯ How will the remediation efforts to limit/repair the damage and restore normal services be prioritized?
- ◯ What special notifications should be prepared for victims?
- ◯ What other actions do your breach notification laws require?
- ◯ What are the legal implications of the incident?

3

Communicate What You Know

- ◯ Here, as elsewhere, bad news does not get better with age, but remember the general rule that the first report is always wrong.
- ◯ Release your initial public statement as soon as you have a reasonable command of the problem and can explain what you are doing about it.
- ◯ Describe what you know so far about what happened and what is being done to correct it.
- ◯ Be prepared to explain the pre-existing cybersecurity posture and the measures that were in place to prevent events of this kind.
- ◯ Be prepared to explain the steps you will take to prevent future unauthorized intrusions. Start with basic cyber hygiene and the CIS Controls.
- ◯ Establish a regular cadence of updates for victims, media, and other stakeholders—including your own workforce.

Headquarters
31 Tech Valley Drive
East Greenbush, NY 12061
+1 518.266.3460

www.cisecurity.org

Need Help?
Call or email the MS- or EI-ISAC
+1 866.787.4722 (24 hours)

soc@cisecurity.org

elections@cisecurity.org

How do I join?
Complete our registration form at

MS-ISAC
https://learn.cisecurity.org/ms-isac-registration

EI-ISAC
https://learn.cisecurity.org/ei-isac-registration

Appendix E: References and Resources

Center for Internet Security®
https://www.cisecurity.org/

CIS Critical Security Controls®
https://www.cisecurity.org/controls/

Council of Registered Security Testers (CREST) Cyber Security Incident Response Guide
https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

NIST SP 800-61 Rev. 2 Computer Security Incident Handling Guide
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

NIST SP 800-184 Guide for Cybersecurity Event Recovery
https://csrc.nist.gov/publications/detail/sp/800-184/final

MS-ISAC® and EI-ISAC® Service: Cyber Incident Response Team (CIRT)
SLTT governments can report incidents to the MS-ISAC Call 866-787-4722 or email soc@cisecurity.org for assistance from the MS-ISAC/EI-ISAC Security Operations Center (SOC) and Cyber Incident Response Team (CIRT)