

State of Oregon Information Security Incident Response Plan

Date: July 1, 2015

Table of Contents

| | |
|---|-----------|
| Introduction..... | 1 |
| Authority..... | 1 |
| Terms and Definitions | 2 |
| Roles and Responsibilities | 3 |
| Program..... | 5 |
| Communications..... | 15 |
| Education and Awareness | 19 |
| Compliance | 20 |
| Implementation | 20 |
| Approval | 21 |

Introduction

Information security incidents affect the state's enterprise information assets and its ability to provide services to citizens of Oregon. Incidents must be investigated and a response prepared to mitigate the state's risk. Because of inter-related data processing and public perception of the State as a single entity, information security incidents at individual agencies may impact other state agencies or the State as a whole. Incident response activities must be effective, coordinated, and protect the interests of individual agencies, the state as a whole, and of the citizens they serve.

The Enterprise Security Office has developed this Incident Response Plan to guide response to information security incidents. This plan is built on the premises that incidents vary in severity and require a flexible scale of response efforts to mitigate, and that response efforts must be adequate, uniform and coordinated regardless of the size. Small, single agency incidents may only require the directed efforts of a small agency team to mitigate, while large, multi-agency incidents may require close coordination between agencies under centralized direction from the DAS Director, the State CIO, or the Governor's Office. This plan presents a response, communications and escalation structure flexible enough to address incidents of any size or scope.

Agencies, in coordination with the Office of Emergency Management (OEM) and in accordance with the Statewide Emergency Operations Plan, are already familiar with incident response in the context of physical emergencies. In order to align with preexisting expertise and incident response structures, this Incident Response Plan was written in close coordination with the OEM and the Emergency Response Council. The Plan adopts National Incident Management System (NIMS) and Incident Command System (ICS) methodology and terminology wherever possible and is designed to fit within existing emergency response practices.

This document describes how resources are to be brought together to respond to an information security incident. The objectives of the incident response plan are to facilitate quick and efficient response to incidents, limiting their impact and protecting State information assets. The incident response plan defines roles and responsibilities, documents the steps necessary for effectively managing an information security incident, describes incident severity levels and how escalation occurs, pre-defines communications channels and prescribes necessary education to achieve these objectives.

Authority

Oregon Administrative Rule 125-800-0020 directs the Department of Administrative Services (DAS) to create a state incident response capability including, but not limited to appointing a standard, multi-agency State Incident Response Team (SIRT). The SIRT is directed to take actions necessary to immediately assemble and deploy the coordinated expertise, tools, communications infrastructure, methodologies and controls required to prevent or mitigate damage caused by an incident. The authority, membership and duties of the SIRT are also outlined in the administrative rule.

Statewide information security policies:

| Policy Number | Policy Title | Effective Date |
|---------------|--|----------------|
| 107-004-050 | Information Asset Classification | 1/31/2008 |
| 107-004-051 | Controlling Portable and Removable Storage Devices | 7/30/2007 |
| 107-004-052 | Information Security | 7/30/2007 |
| 107-004-053 | Employee Security | 7/30/2007 |
| 107-004-100 | Transporting Information Assets | 1/31/2008 |
| 107-004-110 | Acceptable Use of State Information Assets | 10/16/2007 |
| 107-004-120 | Information Security Incident Response | 11/10/2008 |

Terms and Definitions

| | |
|--------------------------------------|--|
| Asset | Anything that has value to the agency. |
| Control | Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, physical, management, or legal nature. |
| Incident | A single or a series of unwanted or unexpected information security events (see definition of "information security event") that result in harm, or pose a significant threat of harm to information assets and require non-routine preventative or corrective action. |
| Incident Command System (ICS) | A standardized incident management approach that allows for the integration of facilities, equipment, personnel, procedures and communications within a common organizational structure; enables a coordinated response among different agencies and entities; and establishes common processes for planning and managing resources. |
| Incident Commander | The Incident Commander has overall responsibility for managing the incident by establishing objectives, planning strategies, and implementing tactics. The Incident Commander is the only position that is always staffed in an Incident Command System (ICS) application. On small incidents and events, one person, the Incident Commander, may accomplish all management functions. The Incident Commander is responsible for all ICS management functions until he or she delegates those functions. |
| Incident Response Plan | Written document that states the approach to addressing and managing incidents. |

| | |
|-------------------------------------|---|
| Incident Response Policy | Written document that defines organizational structure for incident response, defines roles and responsibilities, and lists the requirements for responding to and reporting incidents. |
| Incident Response Procedures | Written document(s) of the series of steps taken when responding to incidents. |
| Incident Response Program | Combination of incident response policy, plan, and procedures. |
| Information | Any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics, including electronic, paper and verbal communication. |
| Information Security | Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved. |
| Information Security Event | An observable, measurable occurrence in respect to an information asset that is a deviation from normal operations. (State) Incident Response Team (SIRT) Team of responders to a State information security incident. Although the makeup of the team may vary depending upon incident scope and severity, it will contain the following common elements regardless of size: an incident command structure, a communications component and information security technical advisors. |
| Threat | A potential cause of an unwanted incident, which may result in harm to a system or the agency. |

Roles and Responsibilities

| | |
|--|---|
| Office of the Governor | Leads state government. The Governor may step in as Incident Commander for incidents Level 3 or 4 depending on scope of incident. |
| State Chief Information Officer (CIO) | Leads state government in enterprise information technology management, strategic planning and policy. The CIO may step in as Incident Commander for incidents Level 2, 3, or 4 depending on scope of incident. |
| DAS Director | As delegated leader of state governmental operations under the Governor, the DAS Director may step in as Incident Commander for |

incidents classified as Levels 3 or 4 depending upon scope of incident.

State Chief Information Security Officer (CISO) Responsible for statewide information security. The CISO may step in as Incident Commander for incidents Level 2 or 3 depending on scope of incident.

Enterprise Security Office (ESO) Responsible for responding to and facilitating response to information security incidents having either multi-agency impact or that are of a severity or scope to pose a hazard to the state as a whole. The ESO monitors and assists agencies with response activities, escalates response activities, provides subject matter expertise regarding information security incident response, and may provide incident command for Level 1 or 2 incidents. The ESO is responsible for gathering agency incident information, aggregating, tracking and reporting on it in a manner that safeguards the security of the agency and state.

Enterprise Technology Services (ETS) As owner of the state network and custodian to much of the state's information, ETS may play an important role in many information security incidents. Although the SIRT has responsibility for handling multi-agency incidents, this responsibility may be shared with ETS for customer agencies and for incidents affecting the State of Oregon network. In technical incidents involving the state network or ETS-hosted equipment, ETS will act as technical lead for incident response activities because of their operational and maintenance responsibility for this infrastructure.

Office of Emergency Management (OEM) Responsible for maintaining the state Emergency Operations Plan and managing the Emergency Coordination Center (ECC) facility. Maintains a state-wide common operating picture and coordinates emergency response and recovery activities across local, tribal, state, and federal governments and the private sector. In incidents classified as Levels 3 or 4, may be called upon to facilitate coordination of response efforts.

State Agency Director Responsible for safeguarding agency information. In Level 1 incidents where the

agency has requested SIRT assistance, SIRT will provide response and advisory capabilities as requested when possible. In incidents classified as Levels 2, 3 or 4, a Unified Command structure may be utilized in which agency directors will coordinate actions and communications with the SIRT and will assist the SIRT in response activities. Agency directors are also responsible representing the agency business owner and for providing business continuity response and leadership in the event a security incident jeopardizes the on-going business operation of the agency.

Agency Incident Response Point of Contact Responsible for establishing agency reporting method and communicating incidents with SIRT. Provides a point of contact for communications between SIRT and agency responders during an incident.

Legal Counsel Responsible for providing legal guidance in all stages of incident response activities.

Public Information Office Responsible for coordinated release of information about incidents to the public, under the direction of the Incident Commander. In the event of a public release and depending upon the scope of the incident, agency Public Information Offices will work together with DAS' and the Governor's Office's PIOs to provide a unified message to the public.

Program

The Statewide Incident Response Program is composed of this plan in conjunction with the statewide Information Security Incident Response Policy number 107-004-120 and procedures.

Rules of Engagement – Agencies will report information security incidents to the ESO within the timeframe specified by the statewide Incident Response policy. Upon being contacted, the ESO will assign an incident coordinator and assess the severity and impact of the incident. The ESO may bring in additional resources and form an expanded SIRT, depending upon incident severity, size and scope. If needed or requested, the SIRT may perform various roles in responding to the incident, including incident command, physical response, forensic analysis, or other roles as needed.

When responding to an incident with an agency, the following are rules of engagement between SIRT and agencies:

- Mutual respect of authority and business requirements.
- Agencies will advise the SIRT of potential incidents in a timely manner.
- SIRT, in conjunction with agency director and business owner, may request or require problem hosts or networks be disconnected from the statewide network and/or the Internet if needed for containment.
- Agency computer resources may be quarantined for forensic investigation.
- Agency director and business owner will actively participate in all discussion that would affect agency business.
- Agencies will provide resources to assist the SIRT to expedite investigations, containment, and resolution of an incident.
- SIRT, potentially including Legal Counsel and Public Information Officer, will work with agencies to determine if, when and how external resources will be notified.
- SIRT will coordinate with agency incident commander(s) responsible for leading business continuity efforts that may result from an incident.
- Agencies and SIRT will maintain clear communications between incident responders.
- Agencies and SIRT will work in accordance with state and agency policies.
- SIRT may require agencies to implement mitigating actions (e.g. patches, firewall rules) in a timely manner.
- Agencies and SIRT will work together on post incident activities such as remediation and lessons learned.

Because of the sensitivity of incident information and the high potential for damage caused by inappropriate release of it, the SIRT will adhere to the following practices regarding agency information:

- Default classification level for all communications within SIRT will be level 3 (as defined in the statewide Information Asset Classification policy 107-004-050). SIRT members will reinforce this message as appropriate with other participants during an incident.
- Information not to be shared outside incident meetings must be identified by agency personnel and will not be included in minutes or any other media that might become public record or be otherwise released.
- Potentially public information brought to the SIRT will not be shared without specific discussion with the agency, Legal Counsel and Public Information Officer prior to authorization and release.
- Information about an incident will not be released to any unauthorized party.

- When it is deemed by the SIRT or ESO that technical details of an incident will benefit other state agencies or the public as a whole, redacted details of the incident will be shared as it is deemed appropriate and confidentiality can be preserved.

Exercises – To test the incident response plan and verify SIRT's ability to execute, information security incident exercise will be planned and conducted as necessary, depending upon the level of recent SIRT activity. Specifically, these exercises will:

- Test the team response using the plan.
- Identify updates to the plan as necessary.
- Verify contact numbers and test communications and escalation.

The SIRT will encourage and assist agencies to exercise their own incident response exercises, including interactions with the SIRT.

Response –

Incident Command – NIMS describes three types of incident command structures:

- An Incident Commander is in charge of directing all incident response activities. This structure works best for incidents that occur under one jurisdictional authority.
- A Unified Command structure, where individuals designated by their organizational authorities work together to respond to the incident. This structure works best for larger incidents that span multiple jurisdictions.
- An Area Command structure, where an organization provides oversight to disparate incident response groups responding to a complex incident. This structure is typically activated if necessary for non site specific, large scale or long-term incidents.

In an environment such as Oregon state government, where agencies are responsible for their own information security but DAS is responsible for coordinating agency response and protecting the overall enterprise, the structure of incident command may vary on an incident by incident basis or in response to changing conditions. For example, response to a severity Level 1, single agency incident may be structured with a single Incident Commander in charge of response. If the incident is escalated to a multi-agency Level 3 status, the Unified Command structure may direct response efforts.

Agency and SIRT incident response must be flexible and allow transition between different incident command structures as part of the escalation process.

Response Team – The size and makeup of the incident response team will be determined by the nature, scope and severity of the incident. Small, Level 1 incidents may require only a few agency staff and minimal or no participation by the SIRT. Larger incidents, especially ones with multi-agency impact, may require a response team consisting of SIRT and agency staff working together. The largest incidents may require extensive use of third party, contracted response resources.

Because response team makeup and size can vary widely, the state must be able to flexibly and quickly increase team size and capability to meet the needs of potentially large incidents. In order to maintain team flexibility and to promote incident response expertise in the state, the SIRT will identify, train and maintain a network of security experts drawn from state agency staff. Similar to a group of volunteer fire fighters, in an incident emergency the SIRT will call on experts from state agencies to assist with response efforts. During response activities these volunteers will be under the direction of the SIRT for all incident-related activity.

Although the bulk of these volunteers will be information security and technical subject matter experts, there are other areas of expertise that are routinely required for incident response. Examples include Public Information Officers (PIOs) and attorneys. The SIRT will identify professionals in these areas, provide training in security incident response as it relates to their fields, and incorporate them into the SIRT as necessary to provide specialized expertise to the team during an incident.

In the event of a very large-scale incident, the internal resources available to the SIRT may be insufficient. The ESO will establish and maintain contractual resources that can be used to hire third-party expertise and capacity to assist with incident response activities as needed. Those resources will include vendors capable of large-scale incident response.

Response Processes - SIRT response activities follow the general incident response handling stages as described in NIST Special Publication 800-61: Preparation, Detection, Analysis, Containment, Eradication, Recovery and Post-Incident Activity. Although detailed description of these steps is outside the scope of this plan, elements of these steps, as they apply to the SIRT's distributed response activities, are described below:

Preparation

In general, the ESO's preparation responsibilities include not only its own preparedness but also assisting agencies in their preparation efforts. Other sections of this document (Exercises, Education and Awareness, Communications) describe aspects of the ESO's response preparedness activities.

Detection and Analysis

Detection of an incident is the process of noticing an event and beginning response to it. An incident is defined as an adverse event and it usually implies either harm, or the attempt to harm the organization. During the course of operations, events occur routinely that must be examined for impact. Those showing either harm or intent to harm may be defined as an incident.

The ESO will have a minimal role in initial incident detection because that process involves analysis of events during the normal course of operations, which the ESO has little visibility into. The ESO will normally become involved with an incident when it is confirmed as such by either agency or ETS incident response processes.

The ESO may receive communications from outside parties that will constitute initial detection – such communications will be passed to agencies for triage.

Triage is the beginning phase of analysis. The objective of the triage process is to gather information, assess the nature of an event and begin making decisions about how to respond to it. When the ESO is notified of a potential or confirmed incident, an incident handler will perform or assist the triage process. Typical questions that may be asked include:

- Nature of the event
- Who is involved in response activities
- What is the scope
- What is the impact and projected impact, including potential legal and press implications
- What containment measures have occurred
- Are there other vulnerable or affected systems

The ESO will assist agencies and other stakeholders in the process of incident identification and analysis if requested.

Containment

Incident containment is critical in the enterprise environment and is a primary concern of the SIRT. Failure to adequately contain an incident increases the scope and impact and is a common trigger for escalation of incident severity.

Containment must include not only reacting to the incident cause itself but also limiting communication about an incident to only those with a need to know. Loss of communications control can easily result in adverse publicity and increases the difficulty of managing an incident.

Eradication and Recovery

After an incident has been contained, it is critical to confirm all threats and vulnerabilities have been successfully mitigated and that new threats or vulnerabilities have not been introduced. The SIRT will assist agencies through the process of verifying eradication was successful and related information is intact and secure before impacted services are restored.

Agency business and IT processes will largely drive incident recovery. The SIRT may provide information security guidance during the recovery process.

Post-Incident Activity

Post-incident activities that the ESO may perform include lessons-learned activities with affected agencies, sharing sanitized incident information with other agencies or external entities for knowledge dissemination, recommending or performing vulnerability assessments or other information security practices, and altering enterprise incident response processes to reflect lessons learned during the incident.

Incident Severity and Classification – Incident severity determination answers the question “**what is the overall impact of the incident on the State of Oregon?**” Accordingly, incident severity ratings drive incident routing, escalation, escalation urgency, and composition of the SIRT to respond appropriately to incidents. Incident severity may change during the course of response activities in response to factors such as scope change, increased publicity or other escalation factor.

The following factors are example considerations when classifying the severity of incidents:

- Criticality of systems that are (or could be) impacted
- Value and sensitivity of the information compromised (if any)
- Number of people or functions impacted
- Political sensitivity
- Press involvement or publicity
- Enterprise impact, including reputational and legal harm
- Multi-agency scope

The SIRT uses the following incident classification levels:

Level 0 – Event Triage.

Upon initial detection of an anomalous event, the agency must determine whether the event is is an incident that requires non-routine incident response activities.

Level 1 - Minor.

Incidents of minor impact that are resolved with minimal disruption of normal activities—there is no need for creation of an expanded SIRT. Incidents with Level 1 impact are the most common. Incident handling activities will be performed by the state agency with minimal assistance from ESO or other state resources. Examples include: miss-mailing of a limited number of sensitive documents, theft of a laptop with little or no sensitive information, and malware infection requiring non-routine mitigation activity. There is little or no likelihood of press involvement and no potential for statewide impact. This is the default, minimum, classification for incidents reported by agencies.

Level 2 - Medium:

Incidents having "hard cost" impacts and requiring nontrivial and coordinated response activity that is not part of normal operations may require the creation of an expanded SIRT. The specific resources required for the expanded SIRT will vary depending on the incident characteristics. Examples of Level 2 incidents include malware outbreaks that impact multiple workstations and/or servers, persistent hacking activity that requires coordinated ESO/agency response, etc. Level 2 incidents may have significant impact to one agency, may require escalation to the SIRT for response, and may have the potential for media coverage. Typically, SIRT's response to Level 2 incidents could include any/all of the following:

- Information Security & Technology Subject Matter Experts
 - Network Administrators
 - Server Administrators
 - Desktop Administrators
 - Application Developers (Dev) and QA
 - Computer Forensics
- Legal Counsel
- Agency Privacy Office Representatives (in cases of Privacy Incidents)
- Agency Business Representatives
- Agency Public Information Office

Level 3 - Major:

Level 3 incidents have major business impact (e.g. incidents involving civil penalties, major privacy breach notification activities, prolonged business disruption, loss of critical services to Oregon residents, etc.) and always require the formation of an expanded SIRT, including possible mobilization of non-affected agency SIRT members. They may be multi-agency with wide spread impact and have statewide press coverage. They may have political impact to State government. Examples of Level 3 incidents include: successful coordinated hacking activity, publicized extortion attempts by hackers, Denial-of-Service (DoS) attacks against significant infrastructure, a database breach and potential release of PII, or a malware outbreak spreading across multiple agencies.

SIRT response to Level 3 incidents could include any/all of the following:

- Incident Command will happen at a top agency or multi-agency level, possibly requiring multi-agency Unified Command
- Information Security, Incident Response & Technology Subject Matter Experts from agencies and the ETS
- Agency Privacy Office Representatives (in cases of Security/Privacy Incidents)
- Agency Business Representatives
- State legal representation
- If criminal, the Oregon State Police (OSP) or other law enforcement

In addition, Level 3 incidents must be communicated to:

- Impacted agency directors
- The Office of the Governor
- Oregon Emergency Management (OEM)
- DAS Public Information Officer (PIO)

Level 4 - Critical:

Level 4 incidents have the highest level of impact to state systems or government and always require the formation of an expanded SIRT commanded at a high level. They may have scope beyond just state agencies (public/private) or be multi-state, may have high impact to citizens, and national press interest. Political impact from the incident could be major. Examples of Level 4 incidents include: Denial-of-Service (DoS) attacks against major infrastructure, terrorist activity, multi-state or national level incidents.

SIRT response to Level 4 incidents could involve any/all of the following:

- Unified or Area Command directed at the highest level: Governor, DAS Director or State CIO
- Information Security & Technology Subject Matter Experts
- Coordination by multiple Agency Directors and agencies
- Coordination with national law enforcement
- Engagement of Oregon Emergency Management (OEM) for command center
- Department of Justice (DOJ)
- Coordinated, strategic Press Communications
- Business Continuity Representatives
- External Subject Matter Experts (e.g. incident response experts)
- State legal representation

The SIRT will classify incidents reported to them according to the criteria above and respond to them accordingly. The SIRT may reclassify and escalate incidents as conditions change and may require agencies to take action based upon the enterprise incident classification.

Escalation – Different level incidents require different types of resources, communication strategies and levels of authority to respond. Incidents and response circumstances may change, often quickly, requiring smooth escalation of response efforts.

Escalation is generally triggered by the following types of events:

- Publicity – Public or Press interest in an incident may increase the sensitivity, urgency and resource requirements
- Scope Change – The scope of the incident may increase
- Responsibility or Authority Change – Responsibility or Authority to respond may be transferred
- Resource Constraints – The capacity or capabilities of current responders may be exceeded
- Political sensitivity – Potential political damage may require a higher-level response

- Perceived or actual mismanagement – Initial response may be (deemed) inadequate, requiring a higher-level response

An escalation requires transfer of authority and incident command to a responder appropriate for the new level of response, including possible transition to a new incident command structure. Additionally, it may require opening communications with other parties, bringing new resources online and coordination with current response activities and personnel.

ESCALATION TRIGGERS

- o Publicity
- o Scope
- o Responsibility/authority
- o Lack of resources
- o Political sensitivity
- o Mismanagement (perceived or actual)

INCIDENT

Escalation and Escalation-Based Communications

Involved Parties

Communication

LEVEL 0

Example Triggers

Initial detection, routine, triage

Agency Incident Response Team

Agency Notifies

- Internal Staff (as applicable)

LEVEL 1

Example Triggers

Agency determines that it meets definition of Incident

Agency Incident Response Team
SIRT – ESO (advisory as applicable)
ETS Staff (as applicable)
No/Little Management Involvement

Agency Notifies

- ESO

LEVEL 2

Example Triggers

Significant impact to 1 agency
Potential or actual media coverage

Agency CISO/CIO
Agency PIO
SIRT – ESO
State CISO
Agency Management (as applicable)

Agency/ESO Notifies

- DOJ (as applicable)
- ESO Notifies
- State CISO
 - State PIO

LEVEL 3

Example Triggers

Multi-Agency, wide spread impact
Significant impact to multiple agencies
Statewide press coverage
Potential for serious impact to state (e.g. reputation, regulatory)

Agency Executive Management (as applicable)
Agency CISO/CIO(s) (multiple agencies)
Agency/State/Governor's PIO
SIRT – ESO
State CISO
State CIO
ETS Administrator (as applicable)
DOJ

ESO Notifies

- Governor's Office
- State CIO (if not already involved)
- OERS to OEM core management

ESO/Agency consider

- Law enforcement (consult DOJ)

LEVEL 4

Example Triggers

Scope beyond just State
Agencies (public/private)
High impact to citizens
National press interest
Serious statewide or multi-state impact

ECC ACTIVATED

Governor Representative
State CISO
State CIO (as applicable)
ETS Administrator (as applicable)
Agency Director (as applicable)
Agency/State/Governor's PIO (as applicable)
DAS Director
TAG – OEM
Governor RPC (as applicable) EO 08-20
Governor GRC (as applicable) EO 08-20
DOJ

ESO Notifies (if not already involved)

- MS-ISAC
- Fusion Center

Communications

Maintaining communications security is critical while responding to information security incidents for the following reasons:

- **Adversarial conditions:** information security incidents are frequently the result of malicious attack. Responders must avoid disclosing information about response efforts that might help attackers. Careful analysis of potential information leakage channels and tight control of information disclosure can be critical. For example, if an attacker has compromised credentials to an email system, relying on that system to communicate about the incident may share information that will help the attacker. Attackers may also monitor public information channels so care must be taken not to disclose information that could help them understand effectiveness of their tactics or state defenses.
- **Reputational harm:** a primary goal of incident response is to minimize the impact of an incident. Damage to the state's reputation can represent a huge impact if an incident undermines the public's confidence in State information systems and personnel. Messaging to the public is a critical component of incident response activities.
- **Information sensitivity:** the subject information involved in an investigation may be sensitive and must be protected appropriately. The incident investigation must not endanger the information it's protecting.

Need to Know - Every effort must be taken to preserve the confidentiality of incidents; for that reason, all communications shall be on a need to know basis. At no time should incident response information be shared unless the recipient has a valid need for it, and careful consideration should be given to appropriate messaging for specific audiences.

Incident Response Team Internal Communications – Because of the sensitive and confidential nature of information and communication surrounding an incident, all communication must be conducted through channels appropriate to the security needs of the information. In general, the ESO considers telephones sufficiently secure for use during incidents and is a generally acceptable method of response team communications. Explicit consideration should be given to the security of electronic communications methods, such as email, to determine whether they are adequately secure for a specific incident. Because of their integration with email, voicemail and faxes should also be used with caution for sensitive information. Information classified as Level 3 or Level 4 must be protected at all times in accordance with the Enterprise Information Security Standards (i.e. encrypted in transit).

Incident Communication – After being notified of an incident, the ESO will determine scope and severity, and then activate members of the SIRT as necessary. Scope, severity and SIRT team membership also determines the participation in incident communications.

Following are the major components of incident communications within the SIRT:

- A comprehensive list of key contacts that need to be regularly updated with status information.

- Contact details for all parties requiring updates.
- The different types of updates that will be required. Different update messages may be required, depending on the level of the incident and the audience receiving the communication:
 - In order to facilitate escalation, potential responders should be prepped before being activated at their severity level.
 - Senior management update (State Chief Information Officer, State Chief Information Security Officer, and State Chief Operations Officer)
 - Legal Counsel should be consulted before any public information release or any consultation with law enforcement
 - Public Information Officer should be prepped and involved in any incident that may involve press communications
 - Agency Chief Information Officer (CIO) and/or Information Security Officer (ISO)
 - Agency Director and Business Owner
- How often each type of update is required and when the next one is due.

Third party notifications may take place in accordance with the following general guidelines:

- To fulfill legal or contractual obligations
- Incident details may be shared with a third party if doing so may help them prevent their own incident
- Involve third parties when they may be able to help incident response, taking care to balance any cost of that help against potential benefits

Press communications external to the SIRT will be handled by the agency PIOs, the Governor's PIO or the Joint Information Center (JIC) if one is formed. Legal council should be consulted before any major press communication. Major components may include:

- Who is authorized to release each different update statement?
- The mechanism by which each update will be communicated.
- A process for vetting information to be disclosed and agreeing upon content
- The different types of updates that will be required. Different update messages may be required, depending on the audience receiving the communication:
 - Impacted agency staff
 - Other State of Oregon staff
 - Update for customers and business partners
 - Press/media statement where required

- Public communication (e.g., social media regarding the status of incident response, written notification following a breach, etc.) where required
- Update for emergency services/authorities

Audience/Recipients – Potential recipients of information from SIRT activities may include:

Office of the Governor: SIRT will communicate with the Office of the Governor to keep the governor informed of any activity that may escalate or may result in a major media event. The Governor may step in as Incident Commander for incidents Level 3 or 4 depending on scope or impact of incident.

Oregon Emergency Management: SIRT will coordinate with Oregon Emergency Management to facilitate coordinated State and local government communications during incidents.

State Chief Information Security Officer: The State Chief Information Security Officer and designated members of the ESO will receive any information they request concerning an information security incident or related matter referred to them for resolution.

SIRT members: Members of the SIRT are also, by virtue of their responsibilities, trusted with confidential information. Others involved in resolving a security incident will be given only the confidential information they must have or they require to secure their own systems.

Other Agencies and Response Teams: Other agencies and response teams, when partnered within the Incident Command System (ICS) during response to a multi-agency incident, will be trusted with incident information to allow them to effectively respond. Information may be shared with agencies not directly involved with incident response activities if doing so will help protect those parties. In this case, information will be limited to what is helpful to prevent further outbreaks or future incidents.

Other State, Local or Federal government agencies and entities: Potential contacts include: US Computer Emergency Readiness Team (USCERT), the state Fusion Center, the state enterprise Business Continuity Team, law enforcement, Homeland Security and the Multi-State Information Sharing Analysis Center (MS-ISAC). The SIRT may share information with these entities to assist in broader incident response efforts but always within the constraints of protecting agency and state interests

Public at Large: The public at large will receive no restricted information. Communication with the public will be closely controlled and monitored by agency, DAS PIOs, or the JIC, as appropriate, and under the advice of Legal Counsel. It is important that PIOs and the JIC recognize that the information made available to State of Oregon employees is in effect made available to the community at large, and will tailor the information accordingly.

Media: The media also are considered part of the general public. PIOs and the JIC will manage communications to the media, with the assistance of the SIRT.

State of Oregon employees: Users of computer systems owned and/or operated by the State of Oregon are entitled to information that pertains to the security of their own computer accounts. Users are entitled to be notified if their account is believed to have been compromised or they may suffer personal loss.

The general State of Oregon user community will receive no restricted information, except where the affected parties have given permission for the information to be disseminated. Statistical information may be made available to the general user community. There is no obligation on the part of the SIRT to report incidents to the community, though it may choose to do so. SIRT may decide to inform all affected parties of the ways in which they were impacted, as well as mitigating actions they should take, or to encourage the affected agency(s) to do so.

External Information Security Resources: The information security community will be treated as general public. While members of SIRT may participate in discussions within the information security community, such as mailing lists, blogs and conferences, they will treat such forums as though they were the public at large. While technical issues (including vulnerabilities) may be discussed to any level of detail, any examples from SIRT experiences will be disguised to avoid identifying the affected parties.

Law Enforcement: SIRT will cooperate fully with law enforcement to provide information that is legally required. SIRT may consult with or request law enforcement assistance in an incident investigation.

State of Oregon Management: Because of the nature of their responsibilities and consequent expectations of confidentiality, members of State of Oregon management are entitled to receive information necessary to facilitate the handling of information security incidents that occur in areas for which they have management responsibilities.

Vendors or manufacturers of involved hardware or software or service providers: The ESO encourages vendors of networking and computer equipment, software, and services to improve the security of their products. To support this, a vulnerability discovered in such a product will be reported to its vendor, along with all technical details needed to verify the problem. Identifying details will not be given to the vendor without the permission of the affected parties.

Vendors, manufacturers or service providers may be a valuable resource to the SIRT for incident response. In this situation, only the information necessary to enable them to provide the desired assistance will be shared. If confidential or sensitive information must be shared, appropriate contractual documents will be executed.

Expertise, Education and Awareness

Responding to an information security incident requires two types of expertise: incident response expertise and information security expertise. General incident responder and emergency response training is applicable and useful in an information security incident, but lack of access to expertise in information security can result in costly and inadequate response efforts.

Enterprise Security Office – The ESO team members are required to maintain professional and subject matter expertise in all aspects of information security, incident response and forensics. The team will identify and attend appropriate training and maintain appropriate certifications.

Agency incident responder training – The ESO will provide or recommend to agency incident responder's basic incident response training covering incident identification and an overview of an incident response plan. Where appropriate, more in-depth training may be provided by the ESO. Additionally, for agencies that will handle other components of incident response internally, the ESO will make recommendations for specific training or courses. The ESO recommends that agencies maintain internal sources of information security expertise as well.

Agency staff identified as resources for SIRT emergency recruitment will be provided incident response training by the ESO. Legal and PIO resources identified as SIRT subject matter experts will be provided training on issues related to incident response within their expertise area.

Awareness – The SIRT also will provide agencies additional education or guidelines in support of incident response activities.

Partner agencies - The success and ongoing effectiveness of the State of Oregon information security incident response plan hinges on an increase in awareness and the on-going ability to respond to cyber-incidents by the Department of Administrative Services and partner agencies. The ability to respond successfully requires high level and on the ground workforce training. Socialization needs to occur in conjunction with the training and training needs to be repeated on an on-going basis for the plan to remain effective.

Contracted Resources – Information Security expertise and resources, although critical for correct response in an incident, may be scarce and in wide demand, especially in a larger incident. The SIRT will maintain pre-approved vendor contracts to facilitate emergency procurement of information security incident response resources.

Compliance

OAR 125-800-0020 directs Department of Administrative Services (DAS) to create a state incident response capability including, but not limited to appointing a standard, multi-agency State Incident Response Team (SIRT). The SIRT is directed to take actions necessary to immediately assemble and deploy the coordinated expertise, tools, communications infrastructure, methodologies and controls required to prevent or mitigate damage caused by an incident. The authority, membership and duties of the SIRT also are outlined in the administrative rule.

The ESO recognizes agencies are subject to additional regulations that require implementing incident response activities and will support agencies in their effort. Some examples of additional regulations are:

- HIPAA requires entities to implement policies and procedures to address security incidents, requires the creation of a security incident response team or another reasonable and appropriate response and reporting mechanism, and breach notification
- The Oregon Identity Theft Prevention Act requires any agency that maintains personally identifiable information to notify its customers if computer files containing personally identifiable information have been subject to a security breach (incident)
- The Payment Card Industry-Data Security Standards requires entities to develop an Incident Response Plan and to be prepared to respond immediately to an incident by following a previously developed incident response plan that addresses business recovery and continuity procedures, data backup processes, and communication and contact strategies

Implementation

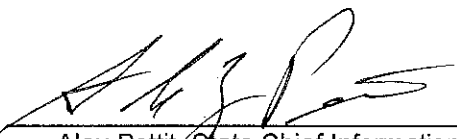
The ESO is committed to assist agencies in formulating and implementing appropriate response strategies. This plan was developed to achieve this goal by giving direction and support for the statewide Information Security Incident Response policy.

ESO will:

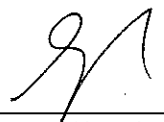
- Respond to state information security incidents.
- Serve as core staff within the Incident Command Structure for incidents classified as Level 2, 3 or 4.
- Maintain trained technical staff with the capability to forensically gather and analyze evidence while observing necessary evidence-preservation practices.
- Maintain a computer forensics lab and perform forensic services for agencies as part of the incident response process.

- Test the incident response plan and verify SIRT's ability to execute.
- Maintain a comprehensive list of key contacts that is regularly updated with status information.
- Provide or recommend basic incident response training covering incident identification and an overview of an incident response plan.
- Make recommendations for specific training or courses.
- Provide education or guidelines on the accurate and timely identification and escalation of incidents.
- Maintain a trained resource pool from agency personnel in order to expand the SIRT team as necessary.

Approval

By: 
 Alex Pettit, State Chief Information Officer

7/27/15
 Date

By: 
 George Naughton, Acting COO and DAS Director

7/31/2015
 Date

By: 
 Stefan Richards, State Chief Information Security Officer

7/27/15
 Date

