Coordinating Response

Foundations of Incident Management (FIM)

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Notices

This material is based upon work funded and supported by the Independent Agency under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

DM19-0875

Purpose

To gain an understanding of the following issues

- identifying and providing an appropriate response
- recording and tracking incident data
- coordinating response with other parties (internal departments, external third parties, other CSIRTs, etc.)
- communicating to a broader audience
- closing and reopening incidents

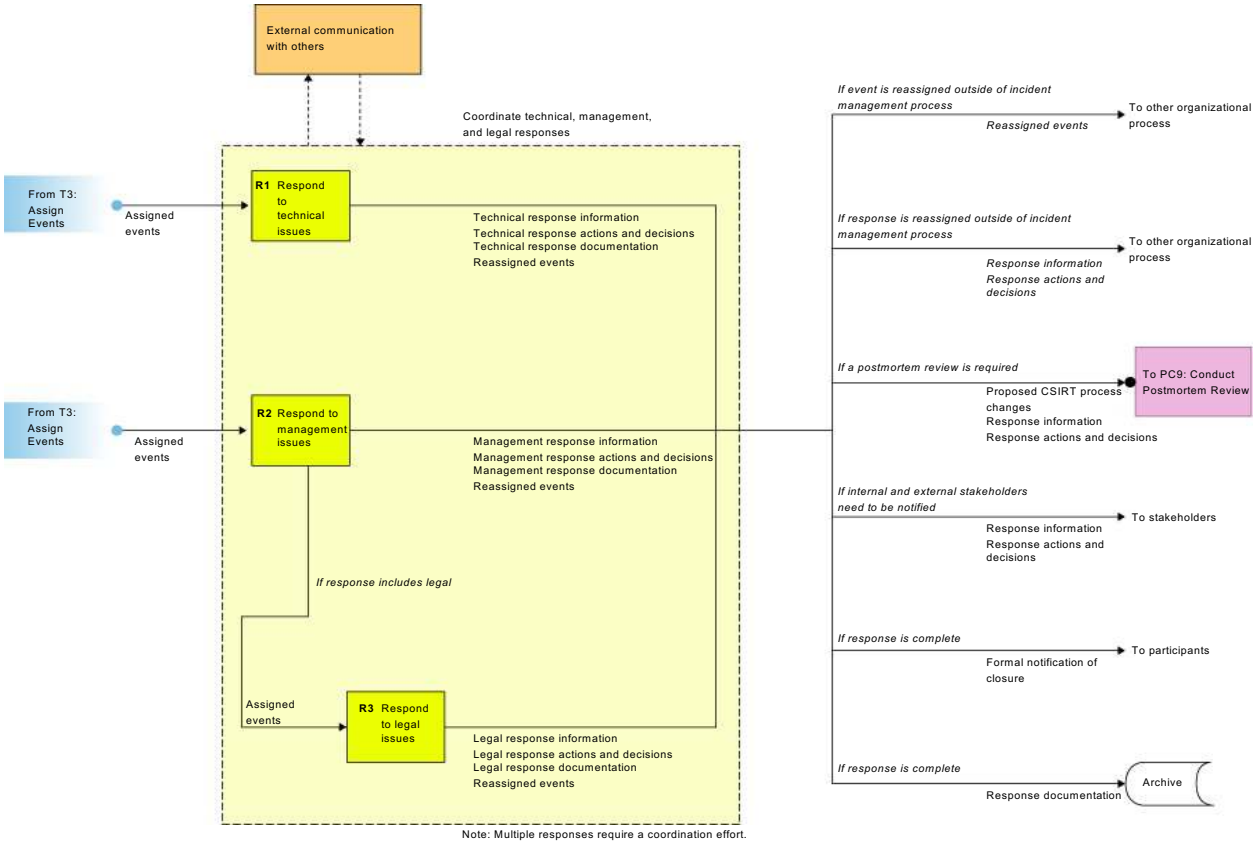
The Respond Process

The Respond process includes the steps taken to address, resolve, or mitigate an event or incident.

We have defined three types of response activities:

- technical
- management
- legal

R: Respond



What Happens During the Respond Process?

Actions can include

- analyzing the event
  - incident analysis
  - vulnerability analysis
  - artifact analysis
  - computer forensic analysis
  - business impact analysis
  - risk analysis
- planning the response strategy
  - determining what steps to take
  - identifying who will need to be involved in the response and contacting them
- coordinating efforts and responding to events or incidents
  - containing and eradicating malicious activity or threats
  - developing and disseminating alerts or notifications
  - making changes in the infrastructure
- communicating with internal and external stakeholders
  - providing updates and briefings
  - closing response
  - passing information to problem management

Response Depends on Your Role

Technical Response

- phone or email technical assistance
- on-site assistance
- data collection
- analysis of logs, files, or other data
- development and dissemination of
  - patches, fixes, workarounds or other solutions
  - advisories, alerts, technical documentation
- feedback to reporting site(s)

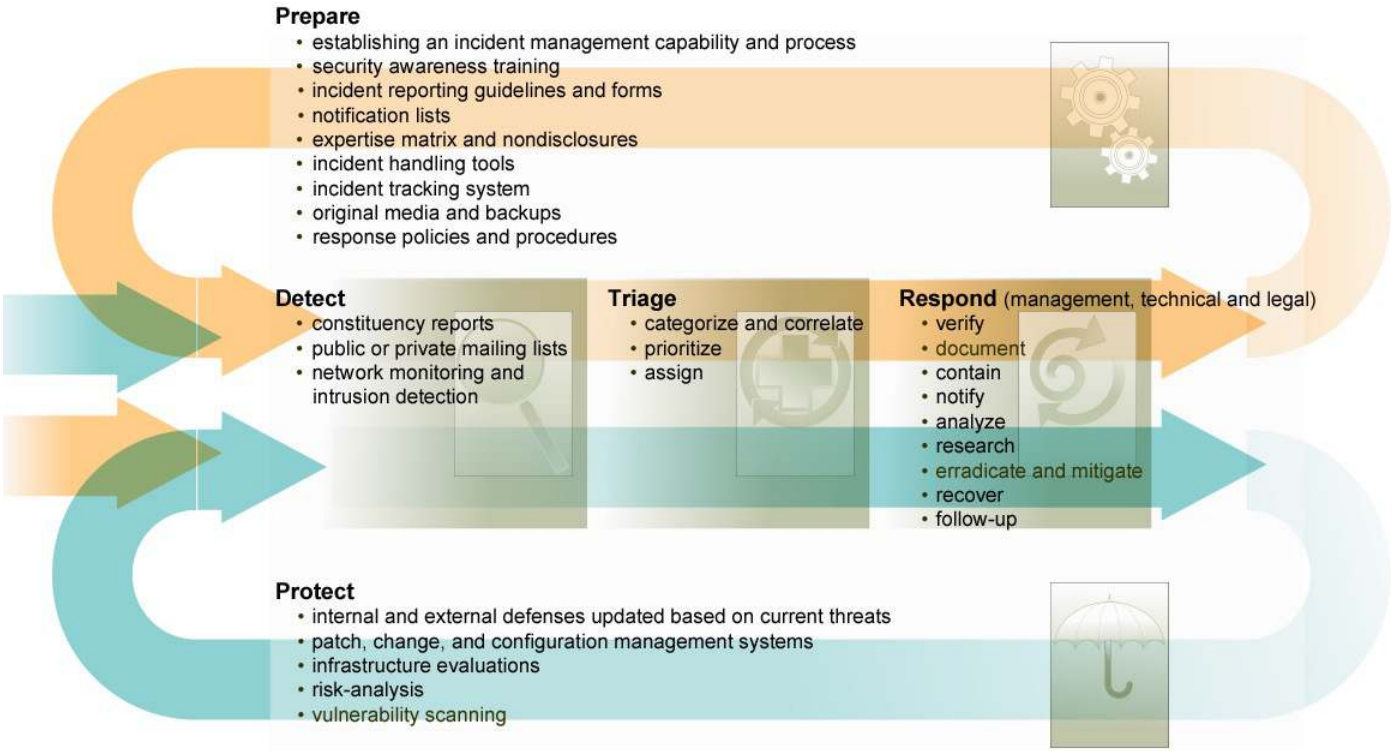
Management Response

- executive or upper management actions
- human resource actions
- media relations actions

Legal Response

- investigative assistance
- legal advice on liability
- review of contracts, SLAs and non-disclosures
- computer forensics
- contacting law enforcement
- prosecution
- compliance reporting
  - contacting affected parties
  - reporting to government agencies

Incident Response Starts Before an Incident Occurs



Preparing for Incidents

To perform incident management as efficiently and effectively as possible, may require other types of activities to be performed.

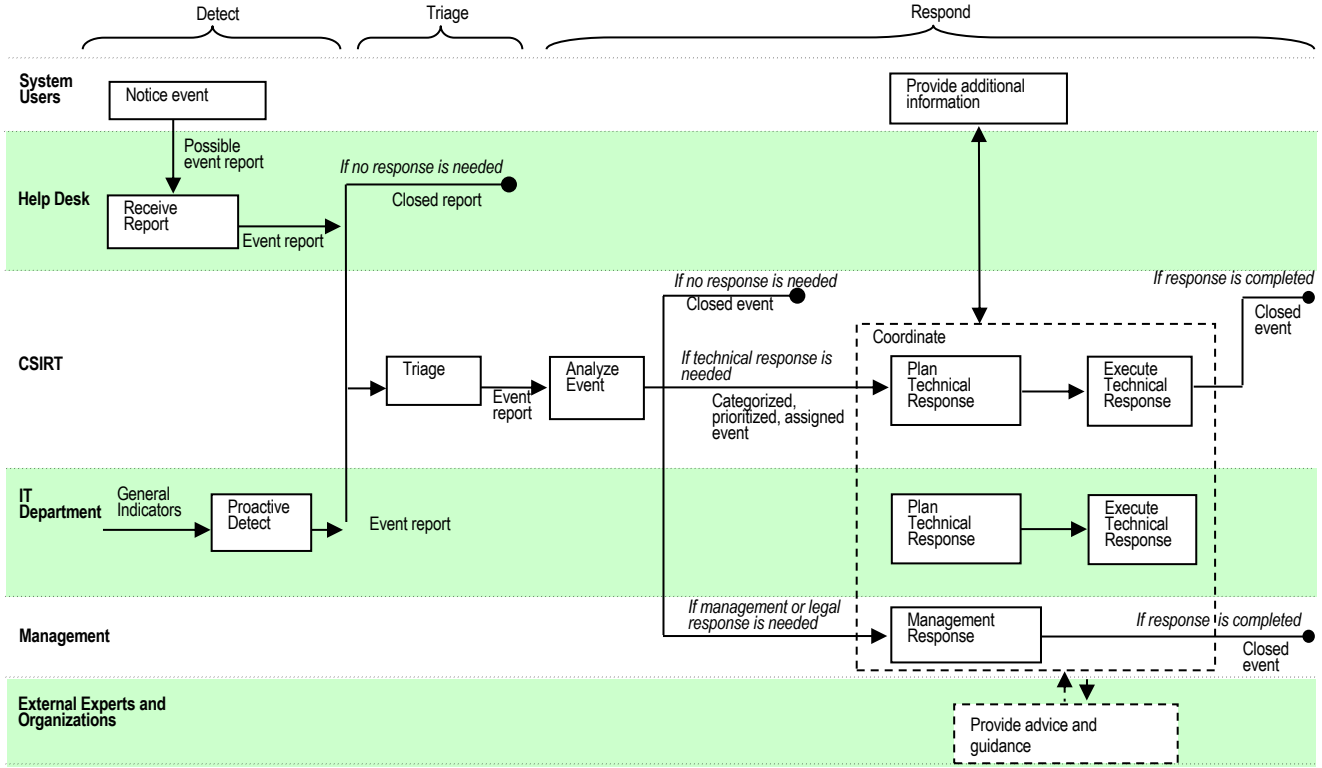
These activities are not all handled by the CSIRT, many have to be instituted by the organization on an enterprise level.

This can include performing

- critical asset inventory and evaluation
- risk analysis
- information classification scheme
- incident management policy and procedure development
- response policy development

It can also include defining interfaces and establishing criteria for when and how to interact.

One Way to Define Interfaces



With Whom Do You Coordinate?

Organizations may coordinate with numerous internal units, including

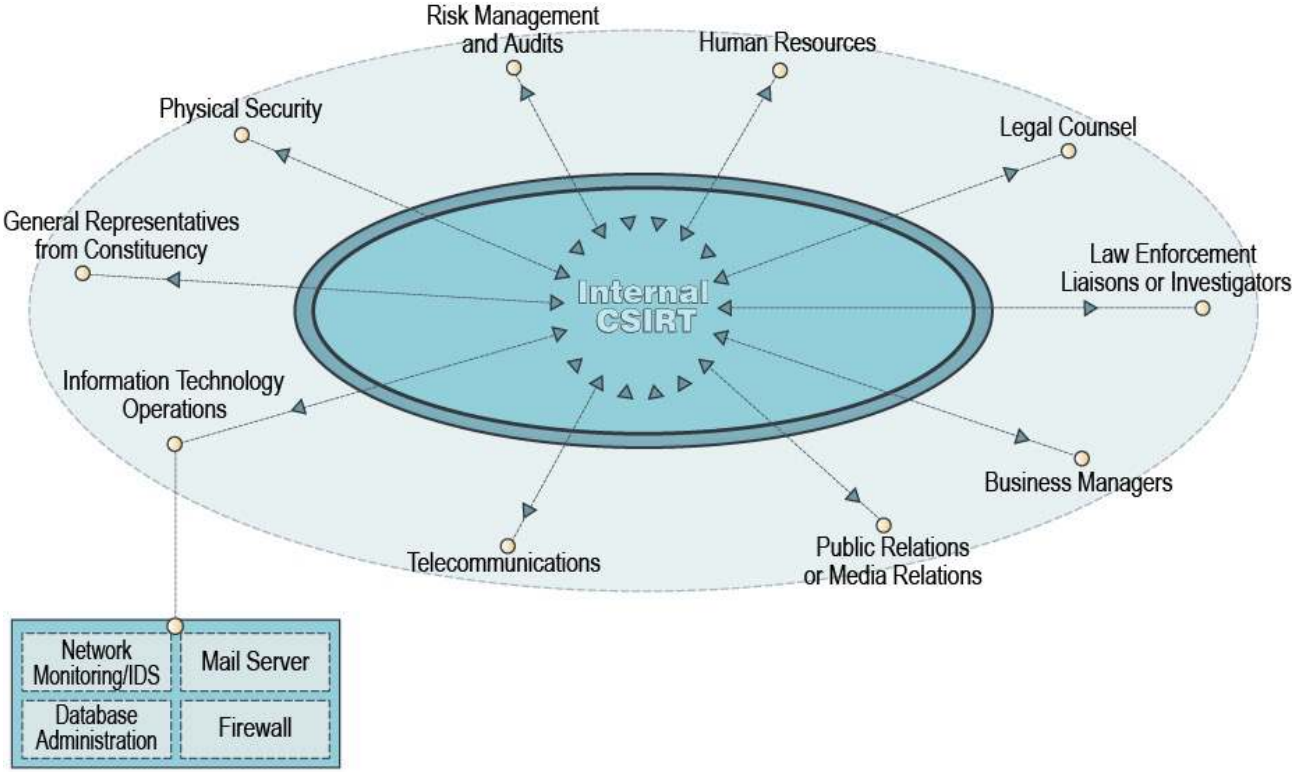
- upper and middle management
- business function managers
- IT and telecommunication groups
- local system and network administrators
- physical security group
- software development groups
- legal counsel
- media relations
- human resources
- internal investigative units
- audits and risk management

Commercial organizations may be legally obligated to contact their customers.

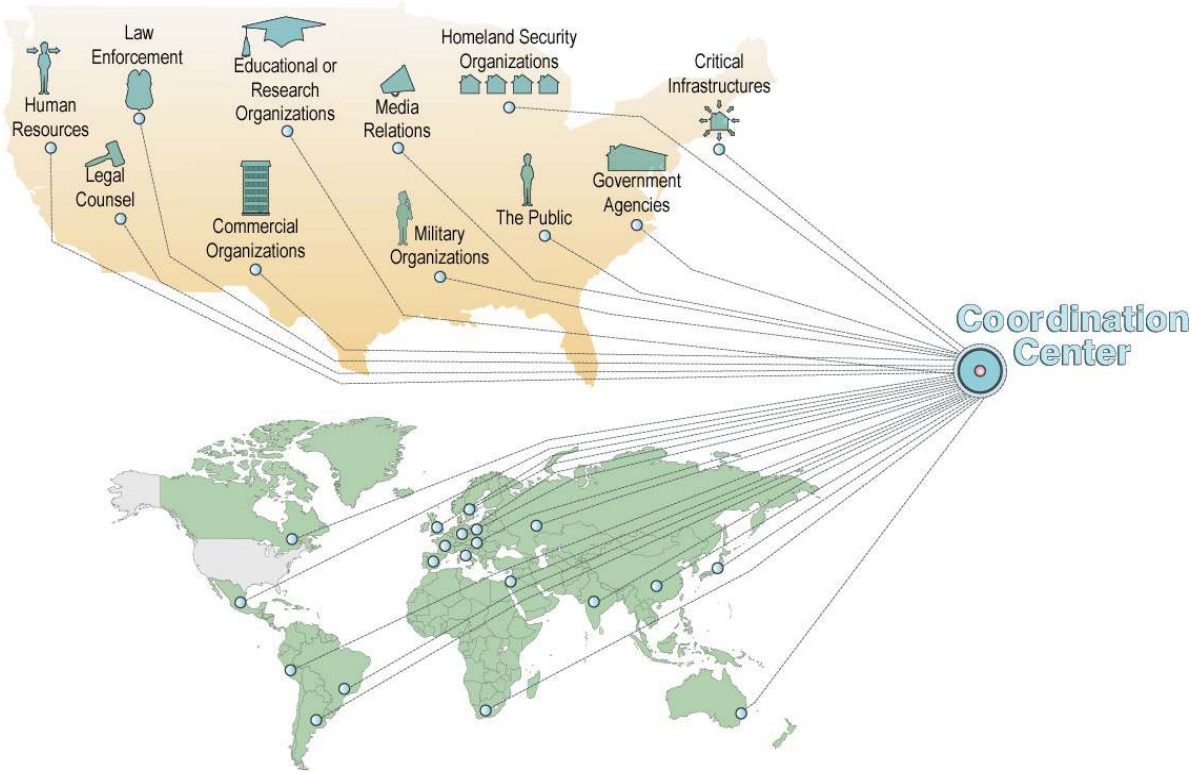
Organizations may also coordinate with external partners, collaborators, liaisons, or other contacts such as

- affiliates
- contractors
- vendors
- ISPs
- law enforcement
- government agencies
- critical infrastructure providers
- information sharing and analysis centers
- national, regional, local, or other types of CSIRTs

With Whom Will You Coordinate?
Internal CSIRT



With Whom Will You Coordinate?
National Team



Coordinating Response

From your CSIRT perspective, understand

- Who is taking the lead for handling the incident?
- Who else needs to be involved?
- How do you contact them?
- Who else needs to be notified?
- How do you contact them?
- Will you need to initiate escalation procedures?
- How are those procedures triggered?
- How will you keep all those involved in responding to the incident up to date?

Coordinating with First Responders

The first responder is the first person to detect an event, incident, or suspicious activity or the first person who arrives to investigate and respond to any detected activity.

First responder procedures and processes must be in place to ensure the consistent and proper initial response to events, incidents or other suspicious activities.

- detectors
- responders

First responders who will not handle the investigation or analysis must be ready to turn over all their information in a clear, concise manner that is easily understood by others.

Documenting Response

Ensure information that is collected and actions taken or to be taken as part of the response are recorded.

This can include

- analysis done
- interviews and discussion completed
- technical, management, and legal response steps taken and rationale
- action items to be completed

Action Items

Document all action items.

Include associated deadlines, if appropriate.

Action items might include

- briefing management or law enforcement
- reviewing logs/files associated with the incident
- identifying sites/teams/others to contact
- finding appropriate contact information
- generating new correspondence or advisories
- disseminating solutions or resolutions

Avoid creating actions that are not under your CSIRT's control.

Contacting Sites Involved

Identify the list of sites to contact.

- Is the site within your constituency?
- If not, then identify which sites have CSIRTs.
- If possible, contact the CSIRTs that represent the sites.
- If there is no CSIRT, you may have to contact them directly, unless a third party agrees to do the contact.
- If possible, contact should be made in a secure fashion.

Caution: Email sent to root, postmaster, or other email aliases at a site that has been compromised could be read by the intruder.

Working with Sites

Provide established contact information.

Encourage the use of encryption.

Set expectations for

- what type of assistance you are able to provide
- what sites should do with the provided information

Working with Other CSIRTs

Use publicly advertised contact information.

Wherever possible

- Use the CSIRT's Incident Reporting Form (IRF).
- Include all incident reference numbers.
- Make use of encryption where possible.
- Set expectations on what the CSIRTs should do with the information you provide.
- Be specific and explicit about the actions you expect/request of the other CSIRTs.
  - Ask "Who is taking the lead?"
  - Request the status of the incident from their perspective.

Disseminating Information

Methods to reach a broader audience

- email
  - creating and distributing alerts and advisories
  - re-broadcasting others alerts and advisories
- via your CSIRT Web page
  - current activity and FAQs
  - technical documents and publications
  - incident or vulnerability notes and advisories
  - blogs
  - podcasts
- recorded messages on phone systems or SMS broadcasts
- XML RSS channels or ATOM feeds (e.g., http://www.us-cert.gov/channels/)
- Social media: Facebook, Twitter, etc.
- press conferences and releases

You may need to use secure faxes, phones, or other secure networks.

Email Issues

When receiving or sending information related to an incident report

- Use standard email headers and signatures.
- Copy your CSIRT alias on all outgoing email for archival purposes to ensure that all email incoming/outgoing to the CSIRT can be tracked.
- Ensure any email sent to an individual account is resent to the CSIRT alias.
- Decrypt internal copies of any encrypted information.
  - These can be re-encrypted with an internal CSIRT key.
- Include all associated tracking numbers.
- Do not include PII information in emails.
- Use secure communications as much as possible.

Closing an Incident

Always inform involved parties when you close an incident.

At what point do you determine an incident is closed?

- Sites may consider incident open until they recover and secure their systems or see no further activity.
- Law enforcement may consider an incident open after CSIRT and sites consider the incident closed.
- CERT/CC closes an incident when unable to provide any further technical assistance to sites involved.

Reopening Closed Incidents

This can occur when new information arrives that is clearly related to a closed incident.

Ensure your CSIRT procedures provide guidance on issues such as

- reopening and reviewing previously closed incidents
- reassigning reopened incidents
- assigning priority to reopened incidents
- identifying reference number usage for reopened incidents

Performing a Postmortem

A postmortem is a review of what happened during the life of the incident, including the detection, analysis, and response processes.

It's main purpose is to identify

- what went right in handling the incident
- what needs to be improved

It can be used to identify

- infrastructure problems to address
- organizational policy and procedural problems to be addressed
- training needs
- unclear or undefined roles, responsibilities, interfaces, and authority
- tools required to perform protection, detection, analysis or response actions

Collaboration

You may have opportunities to collaborate with other CSIRTs or organizations.

- routine information sharing sessions or end-of-shift reports
- joint advisories, tech tips, or other documents
- joint research or analysis projects or incident response
- joint papers or conference presentations
- shared or cooperative training sessions

Secure Communications

When coordinating response, there is often the need to communicate with others in a secure fashion.

This can include situations where

- data breaches and PII are involved
- classified or sensitive data or systems are involved
- an incident is being perpetrated by an insider
- you are working or reporting to external organizations, and are sharing incident data

Methods for secure communication include

- secure email, such as PGP or GPG or S/MIME
- secure web portal, such as the US-CERT portal or secure extranet
- secure phones, such as STU/STE
- secure chat, such as jabber or the chat facility in skype

PGP and CSIRTs

CSIRTs use PGP

- for encrypted communications to/from sites and other teams
- to verify the authenticity and integrity of
  - patches
  - tools
  - announcements and other documents

PGP is the encryption standard used within FIRST.

If you are going to communicate with PGP, try to obtain and verify any collaborator or partner PGP keys ahead of time.

You do not want to be in the middle of an incident and trying to find the keys and verify them, if possible.

What Is PGP?

Public key encryption program

Addresses authentication, privacy, and integrity

De facto standard for encryption of email on the Internet

Not a Mail User Agent (MUA)!

PGP plug-ins exist for many MUAs, including

- Eudora for Windows
- Microsoft Entourage for Mac OS X
- Microsoft Outlook and Outlook Express
- Apple Mail.app
- ICQ Instant Messenger

PGP Principles

A PGP key is actually two unique, matched keys.

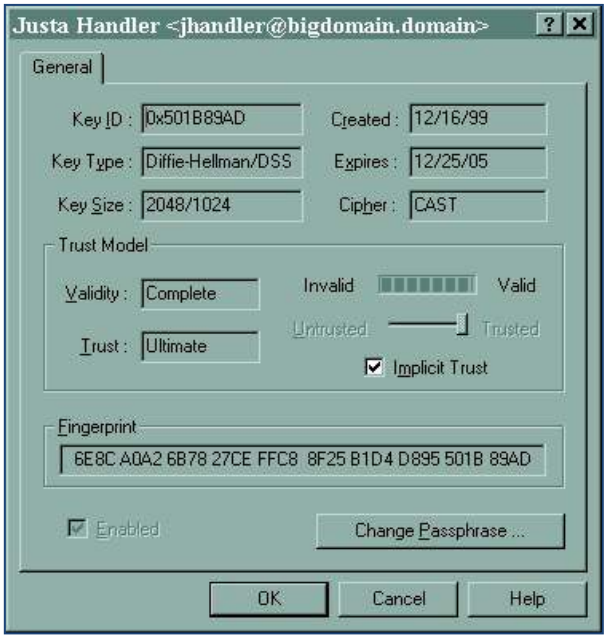
- both created when you create your key (pair)
- work together

Public key

- shareable with the world

Private key

- very closely guarded
- pass phrase protected



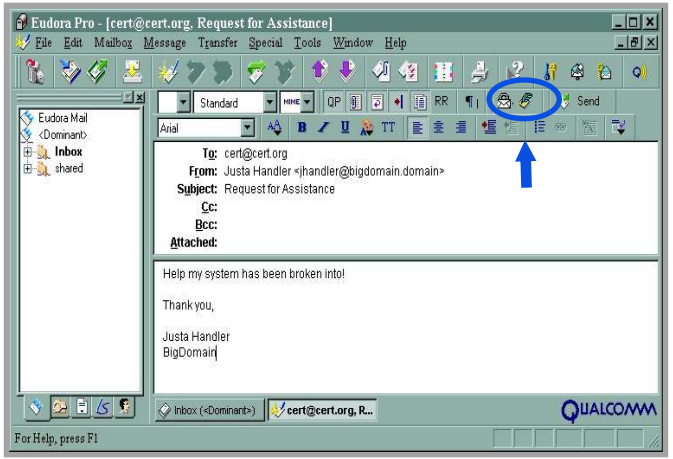
PGP Key Operations

Use your private key to

- sign a message or file
- sign someone else's public key
- decrypt a message or file encrypted with your public key

Use someone else's public key to

- encrypt a message or file
- verify the signature on a message or file someone else sent to you



Key Points

CSIRT work is a team effort—within your team, within your organization, and with many other CSIRTs and sites.

Establish needed communication, notification, and coordination processes a head of time.

It is vital to take time to track and record status and action item information. If you don't think you have time to do it, that is exactly when you should be listing actions.

Determine the best methods to distribute information to those within and outside of your constituency.

Questions