IID Response to NIST CSIC RFI on Document # 2013-15542

SECTION 1 - General Incident Coordination Considerations

1. What does your organization see as the greatest challenge in information sharing throughout the incident response lifecycle?

The perceived risk of sharing information is higher than the perceived risk of not sharing the information. The factors that determine this perceived risk valuation must change.

Organizations who share sensitive information often do not have transparent views into or controls over where that information goes. There are also technical and operational costs associated with setting up the capabilities necessary, and the perceived benefits do not yet outweigh the perceived costs for many organizations.

2. Describe your organization's policies and procedures governing information sharing throughout the incident lifecycle. Also describe to what degree senior management is involved in defining these policies and procedures.

Generally our policies and procedures are as follows. We have more detailed information that pertains on a situation-by-situation basis.

1) Stakeholders who originate information determine what information they want shared with other parties within the groups and the community at large.

2) Stakeholders attribution is anonymous by default unless they choose to announce themselves as the originators.

3) Use automation where necessary and appropriate.

4) Use interpersonal communications in a secure transmission environment where necessary and appropriate.

5) Determine targeted assets, threat assets, stakeholders, and parties who can provide intelligence as quickly in the lifecycle as possible.

6) Coordinate with necessary parties and determine assigned action steps.

7) Evaluate and enhance processes based on shared experience and results achieved.

As we are a company that delivers threat intelligence and incident response to enterprise customers, our senior management is very involved in determining and evaluating policies and procedures.

Please note that IID has a detailed information sharing policy on file. Contact us for more information about this.

3. What role does senior management have in the execution of your policies and procedures?

Senior Management provides leadership, advice, and consent regarding execution of policies and procedures. They take an active role in evaluation of policies and procedures.

4. To what extent is information sharing incorporated into your organization's overarching policies and processes?

Information Sharing is fundamental to what we do for customers every day. Customers rely on us to provide timely, accurate, reliable, comprehensive and efficient cyberthreat information that may be targeting several stakeholders. We serve multiple sectors in this regard and customers use our services to coordinate activities within their own organizations, and also with their supply-chain partners, vendors, and Internet infrastructure operators. In addition, customers use IID capabilities to share information with other parties as a part of their written incident response plans.

5. How much of your incident handling effort is spent on the different phases of the incident handling lifecycle (from NIST SP 800-61): (1) Preparation, (2) detection-and-analysis, (3) containment-eradication-and-recovery, (4) post-incident-activity.

Our organization focuses mostly on the preparation, and detection/analysis and containment/eradication phases, as this is where our value-added

services live for external organizations. We provide assistance and information to customer organizations as they complete the containment and post-incident phases as necessary.

6. What is the relevant international, sector-specific or de facto standards used or referenced by your organization to support incident handling and related information sharing activities?

IID adheres to the standard US-CERT Traffic Light Protocol (http://www.us-cert.gov/tlp) standard for information sharing sensitivity. Our Information Sharing Policy also addresses optional confidence level and activity classifications.

Additionally, IID actively participates in working groups and industry consortia (where such matters are discussed) such as the Collective Intelligence Framework (CIF), APWG, Online Trust Alliance, MAAWG, and ICANN. IID also takes part in the development discussions of various technical protocols for automated threat information exchange such as STIX/TAXII and IODEF and we are adopting the mechanisms that gain consensus within the community.

7. How do you determine that an incident is in progress (or has happened)?

IID is actively searching for cyber threats external to organizations 24x7x365, as well as taking in threat reports from a wide variety of partners. These threat detections and reports are often the first determining factor that a cybersecurity incident is in progress.

Because of the nature of the work we do, our own cyber resources frequently fall under attack. We have several technical and operational mechanisms in place to detect these attacks, analyze them, and respond to them. As we are able, we will share information related to these IID-targeted attacks with external organizations.

8. How do you determine that an incident has been handled and requires no further action?

IID independently verifies and confirms that a cyberthreat is no longer active, in most cases. In cases where we cannot independently verify the

status of a threat (typically due to limited access to internal systems or the nature of the internet infrastructure), we collaborate with necessary parties to ensure a threat requires no further action.

9. How do you determine when to coordinate and/or share information with other organizations regarding an incident?

IID constantly seeks to do this activity as a foundational element of our business. Generally, we look to coordinate with other organizations on an incident when such coordination will aid in faster mitigation of the damage done by a particular threat, and/or will prevent further damage to the targeted organization and to other organizations.

10. Do you have documented case studies or lessons learned to share (good or bad examples)? If so, please provide URLs or attachments with your response.

IID has produced several articles related to this topic, including:
http://www.securityweek.com/brobot-information-sharing-lessons-learned
http://www.securityweek.com/taking-blinders-value-collective-intelligence

Good examples:

IID mitigated the command and control infrastructure of an Instant Messenger worm in 2011. The removal of the command and control domain names required simultaneous action by a dozen domain name registrars located all over the world. IID spent several weeks pre-positioning assets and building the relationships necessary to successfully execute this operation.

IID was also an active participant in the DNSChanger global mitigation efforts in 2011-2012. By alerting organizations of confirmed connections to this malware infrastructure, we were able to help accelerate the pan-industry efforts to eradicate this malware.

Bad example:

The removal of 3322.org (commonly referred to as "Nitol") was an example of an organization (Microsoft Digital Crimes Unit) acting unilaterally with limited coordination with the rest of the cybersecurity community and law enforcement. This action generated negative results in that the organization harmed their reputation in the incident response and research communities,

and eroded their own credibility. In addition, this action caused collateral damage as innocent web sites and services were disrupted and active investigations were hampered. As a result, some industry working groups will intentionally not work with this organization or use mechanisms for sharing that that organization is a member of —a detriment to trust in the community overall.

IID can provide more information on these topics if necessary.

SECTION 2: Organizational Capabilities and Considerations for Effective Incident Coordination

Incident handling teams and coordinating centers often collaborate at varying stages of the incident management lifecycle described by NIST SP 800-61. Within this context, individual organizations may offer specific capabilities and may have specific considerations related to effective incident coordination.

1. Do you maintain a list of key contacts for use during an incident? If so, are these contacts identified as individual people, or as positions?

Yes. These contacts are primarily identified as individual people. In some cases the contacts are email distribution lists to allow for near-real time alert distribution and response. If a key contact is unavailable during an incident, IID will pursue any and all channels necessary to coordinate with a substitute contact for that role.

2. What is the size of your organization (e.g. staff, contractors, members)? How many individuals are involved in incident coordination activities carried out by your organization?

IID has 70 employees. IID has 35 full-time staff members who are primarily responsible for incident response. As needed, this primary team can immediately escalate issues to secondary teams, and in some cases to our executive team as the circumstances may dictate. At least 75% of the IID organization is involved with incident coordination on a more general level: researching current cybersecurity information sharing gaps in and between various sectors, conducting outreach, and building trust and connections where we can.

3. Relative to the incident response lifecycle defined by NIST SP 800-61, what aspects of incident coordination occur within your organization?

For many organizations, IID falls within the Partially Outsourced Managed Security Service Provider Teams outlined in the team models section (2.4.1) of SP 800-61. As our focus is in location and distributing cyberthreats external to an organization as quickly and accurately as possible, our activities touch upon all these areas:

Preparation: In order to prevent incidents for customer organizations, we provide a continuously updated machine to machine feed of confirmed threat locations. Specifically, with the malicious hostnames feed, an organization can apply this feed at their outbound DNS gateway, and harden DNS resolution against communication with known malware hosts.

Detection & Analysis:

We have an expert 24x7 team looking for threats, collecting reports from various sources, and analyzing threats for distribution to external parties.

Containment, Eradication & Recovery:

We publish a real-time feed of malicious URLs for blocking in consumer-facing Internet browsers as part of containment.

With respect to eradication, we work with ISPs, web hosts, registrars, DNS hosting providers, and network and web site owners to remove threats from their assets such as malware drop sites, and phishing pages continuously.

Post-Incident Activity:

We do not primarily focus on this area but do archive our incident response details for future audits and investigations if necessary.

4. What services and assistance (e.g. monitoring, analysis, information) does your organization provide to others both inside and outside your organization relating to incident coordination?

Preparation:
IID assists organizations by consulting with them, alerting them of threat activity that has taken place within their sector or extended enterprise.

Organizations call upon IID for expertise during their strategic planning exercises.

Detection & Analysis:
- IID detects malicious threat presence locations external to an organization.
- IID detects threats that are located within an organization's defined network presence (domains or CIDRs)
- IID detects DNS-related threats such as cache poisoning attacks, or authoritative DNS hijacks.
- IID responds to threat (phishing, malware, etc) analysis requests while organizations are coordinating internal response functions.

5. Does your organization have any method for understanding and describing the quality or sensitivity of different types of information shared by a third party? For each type of information, can you describe the method?

IID has an expert analysis team that examines new sources of threat intelligence and classifies the quality based on a number of factors:

- Pure good: This is intelligence that is high quality and can be incorporated directly into threat intelligence feeds to external organizations.
- Partially Good/Noisy: This is information that is incorporated into processes for threat verification and cleaning. Non-threats are filtered out through these processes.
- Pure junk: This is information that we take in, but is of such poor quality that do not pass along to customer organizations nor continuously verify and clean it.

6. Approximately how many employees (please indicate full time or part time as appropriate) do you devote to incident response?

35 full time staff as part of a 24x7x365 operation.

7. If possible, list examples of highly effective computer security incident response teams and comment on what made them successful.

There have been several such teams that IID has observed and worked with over the years. We can provide more detail as necessary outside of this response forum.

1) Continuous training and active programs to test and drill.
2) Open communications in and between teams.
3) Senior leadership creating an environment of trust and honesty.
4) All team members acting with integrity, and as demonstrated by senior leadership.
5) Post-incident evaluation with active discussion from all involved team members.
6) Procedural information documented and up to date in a secure, hardened, searchable database.
7) Multiple communication channels are used, as the situation warrants.

8. Based on your personal or your organization's experience, what are the most and least effective communication mechanisms used (e.g., phone, email, etc.) when coordinating an incident, and why? In what order do you typically use specific communication mechanisms?

By and large the industry uses email, followed by phone. These are not always the best communication mechanisms. The answer to this question is dependent on a variety of circumstances.

9. Do you have examples of alternate communication mechanisms used because an incident has degraded communications?

IID has responded and coordinated with various organizations during a number of DNS Hijackings over the past several years. Common practice by organizations is often to email a specific team in such instances. In the event of a DNS Hijacking, when the authoritative records are changed for a critical infrastructure domain name, this of course disrupts any email services on top of the domain names in question. IID uses alternate communications channels, such as phone to stand up temporary incident response for organizations under such attack, and our trained analyst team can work with the necessary infrastructure operators to remediate the attack, and get services back online.

10. Do you hold regular incident review meetings? Between organizations? How frequently? If your team does not hold incident review meetings regularly, why not?

Yes. We are in regular weekly contact with customer and partner organizations to drive both day-to-day post-incident discussions and longer-term strategic discussions regarding external threat response. We encourage other organizations to do the same.

11. What skillsets (e.g., network sniffing, system administration, firewall configuration, reverse engineering, etc.) does your organization need most when an incident is in progress?

The examples mentioned above are mostly related to internal incidents on an organization's network. IID provides assistance in the form of threat analysis and as such, reverse engineering and forensics are the areas we most focus on related to this question. IID also focuses on relevant external telemetry – flow data, DNS resolution information, Passive DNS monitoring and indicator correlation, and top traffic generators in the case of DDoS attacks.

12. Are there incident handling and response skillsets that are specific to your industry or sector?

IID is not sector-specific in this sense. We work with organizations from a variety of sectors.

13. How do those skills relate to information sharing and communication before, during and after an incident?

This is on a sector-by-sector basis.

SECTION 3: Coordinated Handling of an Incident

1. Do you report incidents or indicators to US-CERT?

Yes.

2. Do you coordinate incident response with organizations other than US-CERT?

Yes.

3. Do you participate in an incident coordination community such as the Defense Industrial Base (DIB), the Defense Security Information

Exchange (DSIE), or an Information Sharing and Analysis Center (ISAC)? What are the benefits? Are there any pain points?

Yes. IID works with several groups and multiple ISACs.

Benefits:

- Cost Savings.
- Reduced incident cycle time.
- Increased Efficiency in communication workflows.

Pain points:

- Wide-scale information sharing produces significant volumes of noise, a low "signal to noise" ratio, false positives, false flag reports, and the like.
- Lack of current capabilities by many organizations to even begin participation.
- Political infighting within some of these communities creates unnecessary barriers.
- Some of the ISACs are not operationalized for their mission to their respective sectors.
- Other economic sectors not defined as critical still need these communities and capabilities.
- There is a lack of transparency in where and how the information is shared once it leaves the originating organization's hands.
- There is a lack of control over where and how the information is shared once it leaves the originating organization's hands.

4. How is information about threats and/or incidents shared among coordination community members?

Mostly via email and ad-hoc communications. There are some automated information exchanges. The lack of meta-data or context associated with these automated exchanges makes it difficult for receiving organizations to take immediate action upon it. Richly contextualized information is often delayed by days or weeks before the receiving organization obtains it and can take action.

5. How do you prioritize incidents?

We base our prioritization on the impact, severity, and potential harm to organizations we work with. We also look at the immediacy of the threats to organizations we work with every day. For example, a malware command

and control host is prioritized at one level, a phishing site at another level, and unwanted web content at another level.

6. How do regulatory requirements affect your organization's ability or willingness to share information or collaborate during an incident?

We are duty-bound under contract to report information required by our customers, who in turn may be under regulatory requirements to report. We will share cyberthreat information whenever possible.

7. What regulatory bodies are you required to report information to regarding incidents? For each regulatory body, what kind of information does your organization report and what has been your organization's reporting experience?

We are not required to directly report cyberthreat information to any regulatory authority. Indirectly, our customers may be required to report to such authorities. We do archive incident information per standard industry guidelines and for post-incident investigations and audits if necessary.

SECTION 4: Data Handling Considerations

1. What, if any, types of information would create risk or disadvantage if shared by your organization?

IID focuses on sharing actionable threat intelligence and indicators. Risks to IID would include any information that the sharing organization was not authorized to share or allowed to share under law.

2. What kinds of information would you never share with a peer during incident handling?

Personal account information or personally identifiable information related to end consumers where the consumers are not associated with that organization. For example, if an organization shares credit card numbers with IID, we would only share such information with the financial institution that owns those numbers.

3. What types of protections, redactions, or restrictions would aid your organization in sharing information?

Safe harbor provisions would aid IID under law in this respect. Additionally, contractual provisions with sharing and receiving organizations that allow for restrictions in information sharing, and some form of remediation if those organizations shared unauthorized information with other parties.

4. Do you use specialized formats to communicate incident information?

IID uses a variety of widely-accepted formats and transmission protocols, including email, https, .CSV files, XML, JSON, and is also an active participant in working groups focused on emerging formats such as STIX/TAXII.

5. What do you see as the pros and cons of specialized formats for representing and communicating incident information?

These are mechanisms by which machine to machine communications happen. For confirmed, actionable threat indicators, machine-to-machine is one of the best ways to implement real-time network protection at the perimeter and enables organizations to efficiently prevent incidents.

6. What incentives exist for your organization to share information with other organizations during an incident?

IID's core business is to enable cyberthreat information sharing between organizations. Our premise is predicated on the demonstrable fact that when organizations share this information with the community, the information will be more timely and comprehensive than if each organization acts on its own.

7. What disincentives exist that might prevent your organization from sharing information with other organizations during an incident?

Our focus is to reduce and eliminate these disincentives for organizations, so the question is not applicable to IID.

8. If available, please provide an example when sharing with other organizations proved to have negative implications for your organization's incident response.

Not available.