



Information Technology – Information Sharing and Analysis Center (IT-ISAC)

Request for Proposals for Operational Support

About the IT-ISAC

The Information Technology – Information Sharing and Analysis Center (IT-ISAC), is a 501 c (6) not for profit corporation based in Virginia (www.it-isac.org).

Formed in 2000 and operational in 2001, the mission of the IT-ISAC is to:

- Report, exchange, collect, and analyze across the IT Sector information concerning security incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures,
- Establish a mechanism for systematic and protected exchange and coordination of such information and trusted collaboration; and
- Provide technical thought leadership to US and International policymakers on cyber security and information sharing issues.

The IT-ISAC Board has identified three Strategic Objectives that detail the essential value elements that the ISAC provides. The Strategic Objectives are:

- Enable informed risk management by members and partners through effective cyber information sharing and analysis.
- Improve security incident response through trusted analysis, collaboration and coordination.
- Drive informed decision making by policymakers and industry as a trusted sector wide advisor on IT Sector security response and cyber information sharing issues.

The IT-ISAC membership consists of about 20 leading companies in the Information Technology field. The IT-ISAC seeks to continue to expand its membership with industry leaders and expand its core from companies that provide IT products to those who provide IT services as well small and medium sized companies. The IT-ISAC will also begin incremental outreach to international organizations and companies.

The IT-ISAC has identified the following organizational goals toward achieving those strategic objectives:

- Incident Response: Be a trusted forum (through member non-disclosure agreement, collaboration among members, and secure information exchange platforms) for relevant and timely situational awareness-related information sharing on incidents affecting IT-ISAC Members.
- Analytics and Trends: Provide analytics on cyber threat and vulnerability trends and activities
- Provide a trusted forum to work on IT Enterprise and Operations-level cyber security issues
- R&D: Identify R&D requirements and opportunities focusing on solutions to achieve IT-ISAC objectives
- Training and Education: Leverage member expertise and resources to provide best practices, awareness and training to industry and government community. Membership Growth: Expand paid membership to at least 31 companies by August 2012. An operational construct that provides easily articulated value and a clear business case will enable the IT-ISAC to reach these membership goals.

Operational Construct Vision and Mission

The strength of the IT-ISAC is in the collective expertise of our membership. Joint collaboration enables us to see collectively what we might miss individually. A key mission of the Operations vendor will be to drive and facilitate the collaborative analysis—become a coordination point for joint member analysis—including the development of the initial analysis and report drafting that develops these products.

The Operational Construct is designed to meet two main objectives: Facilitating information sharing and analysis among IT-ISAC Members; and providing analysis and alerting around cyber attacks. The construct maintains the ISAC's traditional incident response mission while also meeting members' needs for timely threat analysis that enables them to mitigate risks to their companies and customers. The operational model combines technical analysis with program management, where the Operations contractor produces independent analysis but also serves as a program manager of specific and evolving initiatives that facilitates analysis, information sharing, and risk management solutions among members.

The Operations construct is the coordination point of IT-ISAC operational initiatives. Analysis, incident response, information sharing and member collaboration are all driven by the operational construct.

The mission of the Operational Construct is to provide value to members by:

- Being the definitive resource for information effecting the IT Sector;
- Providing timely alerts of and analysis on cyber attacks including attack data and risk mitigation activities;
- Coordinating and facilitating collaborative analysis and information sharing among members;
- Collating, producing and distributing IT-ISAC products to IT-ISAC members and partner organizations; and
- Serving as a trusted forum and coordination point for member collaboration during cyber incidents.

The IT-ISAC provides value to members both during the “steady state” of daily threats and during cyber incidents. A core component of this value, and role of the Operations construct, is to provide situational awareness to members during the “steady state” and during incident response.

Steady State: Steady state member collaboration is a daily value for IT-ISAC members. Providing daily situational awareness and regular collaboration activities enables members to better identify and mitigate threats to their products and their customers’ networks. Further, as organizations attain daily value from the ISAC, they are more likely to participate in collaborative analysis and incident response.

For steady state, the operational vision endorsed by the Board is a program management model to manage specific initiatives and work streams and to facilitate information sharing and collaborative analysis among members on specific security issues and topics. The IT-ISAC members continue to refine the list of topics for detailed discussion, and it is the responsibility of the Operations team to continue to work with members to identify these topics. An initial list of specific initiatives to be managed will be made available to all vendors who register their interest in responding to the RFP (information on how to register is provided below). This list is non-inclusive and will be increased as new initiatives replace those that have been completed.

Incident Response: A key mission of the IT-ISAC, and essential component of the Operations construct, is to provide core incident management capabilities during cyber and physical incidents that:

- Provides timely incident and threat analysis, as well as suggested risk mitigation activities;

- Serves as a point of coordination and facilitation of collaborative analysis and coordinated response among members; and
- Pushes relevant information to members and partner organizations.

IT-ISAC Partner Organizations

The IT Sector Coordinating Council (IT SCC): As the sector designated Information Sharing Mechanism for the IT Sector, the IT-ISAC has a strong partnership with the IT Sector Coordinating Council, the sector's designated policy coordination body. The IT ISAC and its Members provide technical and operational policy suggestions to the IT SCC. Operationally, the IT-ISAC broadcasts information to members of the IT SCC.

National Council of ISACs (NCI): The IT-ISAC is a member of the National Council of ISACs, which is an organizational structure for collaboration among the sector designated operational entities. The NCI itself is not an operational entity. Rather it provides a forum for leaders and analysts of each ISAC to discuss common issues, share relevant effective practices, identify opportunities for drilling and collaboration, and network. As part of this collaboration, the IT-ISAC facilitates daily cyber and weekly physical calls among the analysts from the members of the NCI. This enables intelligence sources and collectors to identify common cross sector trends, patterns or analysis. The IT-ISAC also organizes out of cycle calls for NCI members during cyber incidents, broadcasts information to members of the NCI, receives analytical products from members of the NCI and participates in conference calls called by other members as needed.

Partnership for Critical Infrastructure Security (PCIS): The PCIS is comprised of the individual Sector Coordinating Councils and includes sector designated operational entities that are not ISACs. The IT-ISAC occasionally broadcasts IT-ISAC alerts and bulletins to PCIS members and organizes calls for PCIS member participation.

InfraGard National Members Alliance (InfraGard): The IT-ISAC operates under a MOU with InfraGard in which it broadcasts certain information to the leadership of InfraGard, for their further distribution to their members.

Forum of Incident Response and Security Teams (FIRST): The IT-ISAC is a member of FIRST. FIRST is a source of intelligence, information and networking for the Operations Analysts. Information received from FIRST is for the ISAC Operations Analyst use. The IT-ISAC can share IT-ISAC generated products, as opposed to member information, with FIRST members, at the discretion of the IT-ISAC Executive Director and/or Board.

The IT-ISAC continues to explore partnerships with organizations on an ongoing basis and often participates in pilot programs and initiatives. The Operations vendor is expected to support these as they become operational.

Request for Proposals

The Board of Directors of the IT-ISAC hereby issues this Request for Proposals for a vendor to assist the IT-ISAC achieve this operational vision. The request is for a two year agreement, with an option for a third year. The Operations vendor will report to the IT-ISAC Executive Director, who is the executive agent of the IT-ISAC Board of Directors. In reviewing the proposals, special consideration will be given to the vendor outlining a vision on how to meet the operational needs described in this RFP. Vendors are also welcome to provide proposals that identify gaps in existing services, capabilities and practices (including IT-ISAC website and member portal), and also explain how the vendor would fill such gaps. The exact statement of work and operational performance metrics will be negotiated with the winning vendor as part of the development of a statement of work.

This Request for Proposal closes at 5:00 pm Eastern on Friday, May 28, 2010 and will be awarded on or about Wednesday, June 23, 2010. **Proposals longer than 100 pages will not be considered.** Other key dates are as follows:

April 23, 2010: IT-ISAC hosted “Discovery Session” with current the IT-ISAC Executive Director and Operations Team on operational elements of the IT-ISAC

April 30, 2010: Deadline for submitting questions relating to the RFP

May 7, 2010: Answers to those questions will be shared with all vendors who registered their interest in answering the RFP

May 28, 2010: Request for Proposals closes at 5:00 pm Eastern

June 8, 2010: Finalize evaluation results

June 15, 2010: Bidders Conference in Miami: Open to Invited Vendors chosen from the finalized evaluation results. Oral presentations about implementation plans and transition plans must be covered during orals. Orals will be limited to 30 minute presentations and 15 minute Q&A. Selected vendors will be notified in their invitation where the orals will be presented.

June 23, 2010: Desired selection date. Vendor will be notified in writing of selection. Contact with Board members related to the development of the RFP during the evaluating period (28 May – 23 June) is prohibited.

July 15, 2010: Transition coordination between vendors begins (if applicable).

August 1, 2010: The new contract becomes effective

Vendors are requested to register their interest in bidding with Scott Algeier, the IT-ISAC Executive Director, at salgeier@it-isac.org. Vendors should designate a primary point of contact so that Scott can be sure that the vendor receives the information it needs to participate in the

Discovery Session and receives the answers to submitted questions. All proposals, and questions related to them, must be e-mailed to Scott Algeier, the IT-ISAC Executive Director at salgeier@it-isac.org. Scott will be the ISAC contact for this process.

Capabilities

The IT-ISAC seeks a vendor with proven program management experience, technical analysis and a history of strong customer service. The vendor must be able to translate complex cyber and physical security issues into valuable analytical products. The ability to aggregate and summarize reports and information, and distributing them to members and partners in an efficient manner is essential. It must have a demonstrated track record of achieving goals of complex organizations, sufficient technical acumen to identify significant cyber attacks or incidents, the ability to quickly generate alerts or warnings of such attacks or incidents, and the knowledge to suggest risk mitigation activities to ISAC members. The winning vendor will need proven incident management capabilities and have surge capacity to respond to incidents on a 24x7 x 365 basis, although staffing is only required during normal business hours. The vendor must submit details on how it plans to provide the surge and out of normal business hours capabilities. The winning vendor MUST be able to foster team work within the IT-ISAC membership, to draw out the member expertise and collaboration in order to assimilate that information into an analytic product for member use and dissemination.

The IT-ISAC has identified three broad operational areas where the ISAC adds value and which the vendor will need to support. These operational areas are:

Broadcast: Consists of simply pushing information out to members, partners and the public, in accordance with our member agreements, Concept of Operations and other agreements/MOUs with security partners. This would include e-mails as well as conference calls. There is no joint technical collaboration in “Broadcast” mode—we’re simply the vehicle for disseminating information. Examples include pushing technical information and information related to patching and remediation tools.

- *Operational Capability Required*: The ability to aggregate and filter information and provide a daily product that is a roll up of multi-source information, with attachments/links with summary products. Steady state rollup of information.
- *Operational Capability Required*: The ability to identify urgent or important issues for members and deliver out of cycle broadcasts to them.
- *Operational capability required*: The ability to build and manage email listservs, the ability to develop, host and maintain a secure web portal and select Out of Band capabilities.

Situational Awareness, Analysis and Incident Response: Consists of the general bi-directional sharing and analysis, at steady state and during incident response, of information about threats,

attacks and incidents in the cyber environment in its broadest sense. Situational Awareness shows what the “environment” is.

- *Operational Capability Required:* The ability to identify, collect, analyze, prioritize, and filter information from multiple sources, including members, and produce and broadcast products based on them.
- *Operational Capability Required:* Provide assessments with analysis, during incidents, at an interval to be determined in a program of work, with the goal of providing timely information, including what to look for—attack techniques, characteristics, forensics—and specific defensive measures that assists members in managing their risks or managing the incident itself.
- *Operational Capability Required:* The ability to securely send, receive and transmit information electronically and via a secure members Portal (see “Key Business Activities Section below) and out of band
- *Operational Capability Required:* The ability to foster team work and collaboration between members and to deliver that input through analytical products and services with regular/periodic updates, and the ability to disseminate select versions of such product to various partner groups in a timely manner.

Collaboration: Is bi-directional technical discussions between the IT-ISAC analysts and members, among IT-ISAC members or between the IT-ISAC and other partners. This includes technical collaborative analysis that provide a better understanding of a threat or incident as well as mitigations. Collaboration generally entails detailed, technical and substantive bi-directional data sharing and analysis. Collaboration provides meaning to information and data.

- *Operational Capability Required:* Drive, facilitate, and program manage threat assessment from across membership
- *Operational Capability Required:* Facilitate, host and program manage specific IT-ISAC technical initiatives, including Special Interest Groups, the Technical Committee and Training and Education programs. .
- *Operational Capability Required:* The ability to provide and manage secure collaboration tools via a web portal, electronic mail, teleconference and other collaborative tools (web conference, podcast)
- *Operational Capability Required:* The ability to foster team work and collaboration between members and to deliver that input through analytical products and services with regular/periodic updates, and the ability to disseminate select versions of such products to various partner groups in a timely manner.

Key Business Activities: Normal business activities that meet the daily needs of the organization. This includes managing listserves, databases, member contact information and responding to member requests.

- *Operational Capability Required:* Proactive and consistent customer service and provisioning support to the Members and partners.
- *Operational Capability Required:* Hosting, managing and credentialing a secure IT-ISAC website (www.it-isac.org)

Specific Tasks

The IT-ISAC has identified the following specific tasks to fulfill each of the above capabilities. A Program of Work agreed to by both parties as part of a statement of work with the winning vendor will provide more details and requirements around these tasks.

Broadcast

The ISAC broadcasts, on a daily basis, information to members and partners in steady state and incident response phases, as detailed in the IT-ISAC Con Ops. These include:

- IT-ISAC Members
 - Technical Committee
 - Member Point of Contact
 - Board
 - Physical Security
 - Special Interest Groups
- IT Sector Coordinating Council
- National Council of ISACs
- Partnership for Critical Infrastructure Security
- National InfraGard Members Alliance
- General public

Specifically, IT-ISAC identified the following capabilities to implement its broadcast mission:

- Maintaining and hosting multiple IT-ISAC Membership listserves, which currently include:
 - IT-ISAC Board
 - Members Point of Contact
 - Technical Committee
 - Physical Security
 - Special Interest Groups
 - Training and Education Committee

- Providing weekly assessments to ISAC Members that prioritize and summarize threats, and linking to sources of additional information.
- Providing monthly assessments to ISAC Members on the threats to the cyber infrastructure
- Organizing secure conference calls, distributing dial in information to partners for IT-ISAC hosted conference calls
- Provide real time web sharing capabilities (live meeting, WebEx, podcasts etc.)

Situational Awareness Analysis and Incident Response

The ISAC desires the following core operational “Situational Awareness, Analysis, and Incident Response” capabilities:

- Identifying, collecting, analyzing, prioritizing, and filtering information from multiple sources, and producing and broadcasting products based on them.
- Collecting and summarizing information feeds and alerts from members, and creating an ISAC product for distribution to members that summarizes and analyzes that information and provides links to the original member submissions for those who want more information.
- Providing assessments with analysis, during incidents, at an interval to be determined in a program of work, with the goal of providing timely information that assists members in managing their risks or managing the incident itself.
- Securely receiving and distributing member threat and vulnerability data
- Managing and facilitating the IT-ISAC Technical Committee, including:
 - Providing a secure phone bridge capability, where access is limited to those invited and attendance on the call can be tracked, for twice a week Technical Committee meetings
 - Taking meeting notes and posting those notes to the Tech Committee portion of the IT-ISAC portal quickly
 - Providing meeting agendas at least 24 hours prior to the meeting [excepting emergent incident response issues]

- Produce and make available, either through the portal or directly with member PoCs a monthly report to each member PoCs detailing the participation of their Tech Committee representatives
 - Identifying relevant security topics and incidents to be discussed at the meetings
 - Summarizing reports and information from other ISACs
 - Facilitate monthly participation from US CERT at IT-ISAC Technical Committee calls
 - Working with the Executive Director, Board and Technical Committee members to identify ways to continually enhance the value of the Technical Committee
- Hosting, with secure teleconference or web sharing tool, and leading daily calls with US CERT and other ISACs to identify common trends, emerging threats and indicators of attacks.
 - Implementing the IT-ISAC Training and Education initiatives and identifying new initiatives as those are completed.
 - Reviewing, on a monthly basis with the Executive Director and quarterly with the Board, the information needs of the members so that the ISAC continues to meet those needs.
 - Supporting and managing a Special Interest Group, if established by the Board, to produce an annual analytical threat report summarizing key threats, vulnerabilities and incidents, and identifying common trends. This includes:
 - Organizing meetings
 - Distribution of meeting notes and next steps
 - Technical analysis to feed the report
 - Report drafting and formatting
 - Managing, testing and drilling IT-ISAC Critical Infrastructure Notification System (CINS), an emergency notification system hosted by the Financial Services ISAC, on at least a monthly basis, to reach members on a 24x7 basis

Additionally, the IT-ISAC has a diverse membership interests that participate in IT-ISAC initiatives. These include physical security, product security, and network security. The winning vendor is expected to identify and present ideas to the Executive Director and Board on how to better meet these needs.

Collaboration

The IT-ISAC has identified the following core operational “Collaboration” requirements:

- Data correlation and analysis of member provided or open source cyber threat or attack information
- Managing various IT-ISAC technical initiatives, including:
 - Identifying topics and recruiting speakers for technical briefings
 - Working with the Executive Director and the Training and Education working group to refine and implement the training and education initiative
 - Managing the Emerging Threat Special Interest SIG
 - Managing other SIGs as they form
- Facilitating member collaboration on the development of joint analytical products
- Facilitate, on at least an semi-annual basis, (one on the east coast and one on the west coast) Technical Committee face to face meetings
- Establishing and maintaining operational relationships with:
 - The National Infrastructure Coordination Center
 - US CERT/NCCIC
 - Sector Specific ISAC
 - The National Council of ISACs
 - International Operational Organizations as determined by the ISAC Board
- Updating with the Executive Director and members, the IT-ISAC Con Ops on a yearly basis
- Participating, as a planner and a player, in up to two full scale and two table top exercises per year, including National Level exercises and Cyber Storm
- Assisting in the planning of and participating in one IT-ISAC member exercise over the course of the two year contract
- Providing secure forums, via an online portal, technical discussions, and direct feeds to members where they can select specific types of feeds they will receive, for the collection and sharing of effective security practices
- Driving implementation of the IT-ISAC Training and Education initiative, including up to 6 podcasts and 6 Webinars per year Providing or making available online meeting, podcast and webinar capabilities
- Supporting the IT-ISAC's participation in the National Council of ISACs

- Supporting the ISAC's participation in pilot programs, as they emerge, including any ongoing or current pilots.

Key Business Activities

The IT-ISAC has identified the following core operational capabilities to sustain key business activities:

- Hosting, managing and credentialing a secure IT-ISAC website (www.it-isac.org). Vendors are expected to propose a security plan to comply with ISAC Member/Non - Disclosure agreement as part of their response to this proposal, that are comparable to NIST Electronic Authentication Guide's Level 3 Assurance (http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf#51).
- Providing current and relevant information to the secure members' portal and updating the website daily with security related news feeds
- Changing the content of, or posting additional content to, the IT-ISAC.org website within 24 hours of the request by the Executive Director
- Providing "on call" staff to enable a 24 x 7 response capability and a surge capacity to manage incident response
- Responding to member requests, and those of the Executive Director, within 24 hours of receiving the request for steady state, and within two hours if the ISAC is at Threat Level 3 or higher.
- Maintaining and updating, on a monthly basis, a list of 24 x 7 contact information for the following set of ISAC members:
 - Board of Directors
 - Up to two Technical Committee representatives from each Foundation member company
 - One Technical Committee representative for each non Foundation Member
 - Up to two Member Point of Contacts for each Foundation member company
 - One Member Point of Contact for each non Foundation member
- Maintaining and updating, on a quarterly basis, the IT-ISAC Critical Infrastructure Notification System, which is hosted by the FS-ISAC.

Other Considerations

The IT-ISAC has provided a vision for its operational construct. As vendors consider their response to this proposal, they are encouraged to share their opinions on how the IT-ISAC can provide operational services that meet these operational goals in an efficient manner. The IT-ISAC is looking for a vendor that provides clear ideas on how it will be an active partner in meeting this vision.

The IT-ISAC is a dynamic and evolving organization. Innovation is an accepted practice in this RFP. Membership needs are constantly evolving, as is the nature of the threat. Understanding and meeting these needs is a core component of the Operations construct. The operations vendor must therefore develop and maintain trusted relationship with ISAC members and leadership, and be willing to adjust products or services to meet these changing needs.

The IT-ISAC is looking to fund the operations construct in an efficient and cost effective manner. Therefore, vendors are asked to propose innovative and cost effective models for funding the Operations Construct. For example, times and material, set fees, and separate fees for data feeds and operational staffing, or additional models proposed by vendors, will all be considered.

This RFP references the IT-ISAC Con Ops, the member agreement and the Training and Education initiative, which are IT-ISAC confidential documents. They will be provided to vendors who request them in order to enable them to submit proposals. By voluntarily participating in the RFP process, vendors who receive these specific IT-ISAC documents agree to use such documents for the sole purpose of responding to the RFP. These documents can be shared only with employees and subcontractors, if any, who are directly participating in developing a response to this RFP. Any misuse of these documents by a vendor will result in that vendor's proposal being rejected and is subject to further action by the IT-ISAC.