Response to Department of Homeland Security, Notice of Request for Public Comment Regarding Information Sharing and Analysis Organizations

DHS Docket No. DHS-2015-0017

July 10, 2015

Submitted by: ICF Incorporated, LLC

POC: Greg Frank
Vice President, Identity Management & Cybersecurity Solutions
gregory.frank@icfi.com
443.573.0540

9300 Lee Highway
Fairfax, VA 22031
info@icfi.com
703.934.3000
703.934.3740 (f)
www.icfi.com

DUNS: 004853412
TIN: 52-1209369
CAGE: 2X091

Executive Summary

ICF International (NASDAQ:ICFI) provides professional services and technology solutions that deliver beneficial impact in areas critical to the world's future. ICF is fluent in the language of change, whether driven by markets, technology, or policy. Since 1969, we have combined a passion for our work with deep industry expertise to tackle our clients' most important challenges. We partner with clients around the globe—advising, executing, and innovating—to help them define and achieve success. Our more than 5,000 employees serve government and commercial clients from more than 70 offices worldwide. ICF's website is www.icfi.com.

A Leading Force in Energy Infrastructure Protection: As threats to the energy infrastructure continue to increase, ICF supports the agencies responsible for grid protection and cybersecurity providing analysis, risk management, and resilience strategies. ICF contributed to vital grid protection efforts with continued support of the U.S. Department of Energy (DOE) and the U.S. Department of Homeland Security (DHS). ICF helps DHS make mandated updates to its National Infrastructure Protection Plan – a plan ICF has been involved with since its inception in 2003. ICF staff provided analysis and recommendations concerning the new Presidential Policy Directive (PPD) on National Preparedness, particularly the National Protection Framework.

A thought leader in Cyber Research: ICF supports two of the nation's premier Research Laboratories by providing innovative staff and ideas that are being utilized today to defend our nation's IT infrastructure. We are thought leaders in the development and implementation of defensive tools in cyberspace, with positive results both within the research community and the government-wide cyber defense community.

Introduction:

ICF is pleased to offer comments to DHS on Executive Order 13691 and public formation of Information Sharing and Analysis Organizations (ISAO) for cybersecurity information sharing. ICF's experience in cutting edge cybersecurity work is complimented with our development and support of information security programs for underserved communities enables us to provide the following recommendations.

ISAO: Take a good start further; get the information right, then keep going.

If alive today Benjamin Franklin may amend his statement about the world's certainties. Death, taxes and information technology. Information Technology has allowed business to make unprecedented gains in production, communications and operational efficiencies. Technology is pervasive in our personal, private and business lives.

Organizational reliance on technology has made us vulnerable to cyber threats. The gains, innovations and advancements are being unfairly limited by the costs of shielding of our assets and operations. Each innovation in virtualization, mobile computing and cloud innovations uncovers new cyber battlefields.

Cyberspace is not constrained by boundaries, boarders, sector or regions. The emergence of cloud computing and shared service providers blur the lines of delineation and responsibility.

With this IT revolution and all its advantages emerges new and unanticipated threats to security and privacy.

The adversaries we confront today are not the proverbial pimple faced miscreant in the basement aiming to deface a web page. The adversaries of today are intelligent and wield sophisticated tactics, techniques and practices. Our adversaries are making coordinated and deliberate attempts to commit industrial espionage and to acquire intellectual property. Our adversaries exist within and without our boarders, our networks and our buildings.

We no longer have the luxury of underestimating their capabilities or justification for applying anything less than our best collective resources to defend our assets. The challenges demand solutions that are collaborative, maturable, sustainable, and evolve to a degree that the capabilities and advancements themselves are a deterrent. Our intelligence gathering techniques and defense must be comprehensive, holistic and span all landscapes both horizontally and vertically.

> The purpose of this order is to encourage the voluntary formation of such organizations, to establish mechanisms to continually improve the capabilities and functions of these organizations, and to better allow these organizations to partner with the Federal Government on a voluntary basis.
>
> *Federal Register*
> *Vol. 80, No. 34*
> *Executive Order 13691 of February 13, 2015*

With this view President Barak Obama signed and released Executive Order 13691 – Promoting Private Sector Cybersecurity Information Sharing on February 20th. The president's order charges DHS with prompting commercial organizations to establish self-governed communities for the purpose of cyber-related information sharing.

Information sharing communities is not a new idea. Sector specific and mainly critical infrastructure Information Sharing and Analysis Centers (ISAC) have been operating for more than a decade. Preceding this executive order dozens of non-critical infrastructure or non-sector specific Information Sharing and Analysis Organizations (ISAO) have been created.

This Executive Order compliments established information sharing networks and aims to officially define and establish a structured framework to share information for smaller organizations with common interests.

ICF believes this is a good next step in bringing cohesion to this underserved community and invite them to address the common problems which concern every area of commerce, science, education, communication and government entity. Coordinating efforts, ideas and strategies is the only way to channel the best of all knowledge and capabilities to match the magnitude of the threats before us.

However, while we support this first step, we believe there are greater gains to be sought by this initiative. It is necessary to go beyond sharing information and lay a path to allow for enhanced services and advanced collaboration.

Requirements for a Maturable Cybersecurity Eco-system: Trust, Valued Services, Serve Your Community

<u>Trust</u>

It may be self-evident and it has certainly been stated several times during the DHS ISAO public forums and outreach, however, it is also worth repeating so that it remains the central theme of our communal sharing of information. The first step to fruitful collaboration and information exchange is trust.

How do you build and scale trust? This is not an easy question to answer. Given the nature of the current cyber climate, the recent occurrences of cyber breaches on private and public systems and controversies related to national data collection programs, private businesses are reluctant to engage in open and full cooperation regarding their most vulnerable cyber information.

In order to be successful ISAOs and DHS will need to overcome the concerns of their ISAO community members. ISAOs must remain cognizant of each conduit of trust and the various perspectives required to establish healthy and functional relationships. Fractures in any link in the relationships between DHS, the Standards Organizations, the ISAO community leaders and the ISAO communities' members could limit ISAO participation and undermine the program's success.

Each ISAO community, be it communication providers, retail stores or small consulting firms, will have a distinct definition of confidence. Each will insist information sharing methods and data stewards handle their sensitive information with care and diligence.

ISAOs will have to establish means to protect the sensitive information of their community. Protections such as disclosure protocols, encryption, and anonymization should be employed. The means and practices should be consistent with the ISAO community member's need for confidence.

Valued Services

It is important to remain aware of the risks and impediments that could undermine the exchange of information and obstruct the path to more valuable and mature cybersecurity collaboration.

First and foremost, ISAOs should make sure the information they assemble and distribute is accurate, valuable and actionable. However there is a trade off when sharing information between organizations.

Information including indicators of malicious activity as well as information that is specific and unique to a particular environment (such as network or server configurations), and the information that resides on those systems, could yield very detailed information about threats such as: their common targets; vulnerabilities they specifically exploit; and methodology. This information can be considered extremely sensitive to partner organizations, making the information difficult to distribute. Organizations may simply not share specific, possibly important, information or dedicate significant amount of work hours to anonymize or redact this information; thus reducing its usefulness.

Another major issue when sharing information includes personally identifiable information (PII).

This should not be shared outside of the organization trusted to protect this data. Data needing to be shared between organizations will either need to be removed, or at the very least anonymized or obfuscated, to prevent the attribution of this information to specific people. Similar to other sensitive information, this effort could require significant work hours.

When establishing a partnership with an ISAO, an agreement will be required to clarify the responsibilities and protections each organization will perform in order to maximize the relationship's value. The partner organization will need to pass information to the ISAO in order to share it with other partner organizations. If an organization will not send raw or anonymized information, the responsibility of performing the analysis and determining the different threat factors will fall on that organization. While most organizations are not by their nature versed in the analysis of threat data, the ISAO can provide the information, methodology, and perhaps training necessary for a partner organization to dedicate a few of its personnel to collecting and analyzing threat information.

In another example, a potential partner organization may not be interested in performing its own analysis and rely on the ISAO to perform this function. This would require an ISAO and member organizations to establish mechanisms to securely transmit threat information. Using the Traffic Light Protocol [i]or similar methodology, partner organizations can label outbound security information to an ISAO utilizing specific sensitivity levels defining how the information itself, and the derivative information may be shared with other organizations. However, it will be the ISAO's responsibility in utilizing the proper protection needed to ensure that information is only shared in such a way as identified by the owner. In this example, the ISAO will receive information in a timelier manner, and the partner organization must now trust the ISAO to secure its information.

Regarding to the dissemination of threat information, ISAOs should quiet the noise. There exists a myriad of public and private sector information providers distributing information about emerging threats. This information is often duplicated, leaving end-of-line organizations with the burden to sort, correlate, and examine the information in order to take action. This process delays response times. ISAOs should ensure the data being collected or provided is not so voluminous that it becomes burdensome for participants to find the elements useful to them. The data should stick to the key concept of what the sharing effort is about and not include specialized data points that will benefit only a few. Collect and provide the data that truly interests participants and participation levels will increase naturally.

Serve Your Community

The endeavor of establishing an ISAO may not be a for-profit venture, however there are entrepreneurial approaches each ISAO should adopt. ISAOs should consider their members to be customers. ISAOs should make efforts to understand their community constituents, their challenges and solutions they seek. ISAOs should commit to regular outreach, surveys and related methods to ensure the ISAO understands their customer's unique needs and the performance gap being addressed.

This formal designation of an ISAO allows for the government to entice participation with incentives and protections not otherwise afforded. DHS and ISAOs should open discussions and seek to offer tax incentives, legal protections and other measures to entice commercial

organizations into participating in information sharing programs. ISAOs could benefit from guarding their customers from liability, which would encourage their participation in data exchange and related collaboration.

ISAOs will naturally assemble to meet their specific needs, their unique challenges and circumstances. However, critical mass remains important. ISAOs should seek out advocates and key members to help proselytize the message. ISAOs need to have clear service objectives and know participation levels, cost of services, associated costs and a fee structure to support the institution.

A Pathway to Advanced Services

Mike Echols, the Director of the Joint Program Management Office at the Department of Homeland Security, Cybersecurity and Communications stated "This ISAO Executive Order intends to provide an opportunity for those groups that don't fit neatly into sectors to come together to perform analysis and to share information." He also said, "They [ISAOs] represent an opportunity to open a pathway for new entries; for new players to come on the field and to train their own players."

For many organizations this executive order will open their first foray into cyber security collaboration. Organizations that previously lacked an understanding of the threat information or lacked the capabilities to make use of the information are now invited to sit at the table. However there are inherent constraints that could inhibit their participation in ISAOs specifically because the ISAO target members are often small and medium sized businesses (SMB) or otherwise under-served organizations. These organizations may not recognize the value and importance of cyber information sharing. They may lack the ability and resources to turn the cybersecurity services into actionable information. Given the target of the ISAO initiative it would be wise for DHS and the selected standards organization to promote ISAO services which would provide the greatest capture of small and medium size businesses.

While individual budgets and capabilities may be modest, the SMB community can collectively leverage a common platform, shared resources and knowledge to equip themselves with the necessary tools to match the needs.

ICF created and currently supports programs which provide information security, vulnerability assessment, education, training and incident management for a community of small businesses that otherwise would be unable to assemble the essential resources and capabilities to properly protect themselves from common cybersecurity threats. Using the lessons gleaned from our experience with similar communities, and similarly constructed models, ICF recommends the following areas of attention for DHS and the to-be named standards organization to take into consideration.

While we enumerate several preliminary services here, we advocate each ISAO initiate out-reach with their community and potential community members to determine which services are most suitable for their constituents.

ISAOs should establish services to enable smaller and underserved communities to access the ISAOs offerings such as:

- Entry level service offerings - Offer services that provide advice, advocacy and consulting services, so that underserved and small business candidates can evaluate and leverage their resources to participate in the ISAO initiative. Services should focus on SMB ISAO onboarding technical and operational preparedness and related advice.
- Contracting vehicles and common services - ISAOs should use their role to establish formal relationships with key vendors, technical consultants and services so that smaller organizations can access via discounted prices on necessary products and services otherwise unavailable to them.
- Establish regular reoccurring information forums to exchange threat trends, best practices, methodologies and related topics.
- Establish a workforce development program to build capacity and capabilities in the areas of forensics, research, operations and development. Use Research and Development (R&D) projects, mentorships and hands-on exercises as an opportunity to develop next generation cyber leaders.
- Leverage tools and subject matter experts to assist under staffed and constrained organizations with Information Security Policy Development and Compliance activities.
- Promote the formation of self-sufficient cyber-mentoring programs. Partner SMBs with larger organizations that have mature information security practices to accelerate the SMB cybersecurity maturation and avoid common learning curves.

Going Beyond Information Sharing: Research and Development

There are millions of dollars being spent by private and public organizations on cybersecurity and yet all indicators suggest that our digital infrastructure is not as safe and secure as our efforts would suggest. The risks are evolving, the actors are evolving and so must our response.

The adversaries who wish to disrupt information technology and business operations are mature, often well-funded and coordinated. Their aims are not solely to disrupt and annoy but are motivated by national interest, commercial competitiveness and theft of real assets. The attack landscape and the methods and means are fluid. The risks to our national and collective security are greater than can be mitigated by reactionary countermeasure-based solutions.

We cannot afford to wait for a cyber-pearl harbor before we mobilize and put forth our best collective effort behind our common problem.

It is not enough to share information about today's cyber threats. Information and preparation provide more effective ways to find the needle in the haystack but fall short of deterring the next attack or preparing for the one after that. We need to stop looking for the needle and start building magnets.

And while there is good science-based cybersecurity experimentation taking place across the academic and commercial landscape, too often the research is stove-piped and cannot adequately address narrowly focused topics. This narrow focus often leads an uneven results.

The magnitude and complexity of the issues call for a concerted and committed effort from every player on the digital grid in our nation. The release of this executive order lays the foundation to

develop an R&D framework needed for a sustained, coordinated effort among a wide and diverse collection of organizations and government partnerships. It is beneficial to *design-in* an R&D framework in the early stages of ISAO standards development. DHS, the standards organizations and ISAOs should make every effort to maximize this extraordinary opportunity to encourage community wide collaboration in order to confront underlying vulnerabilities common to future ISAO communities.

It is more than a good idea. To assemble a collection of organizations that share common threat vectors, aligned business practices and objectives, common stakeholders and yet do not take full advantage of the common resources and motivations for the best possible results would squander this unique opportunity.

Government, commercial, business and education sectors need to prepare for tomorrow's threats and have the technology available to deploy against these emerging problems. Our collective national interest demands trustworthy and reliable computing infrastructures. We must turn the tide, get out in front of our adversaries so we have better protection from their malicious intents.

The president's proposal provides a unique platform to unite the efforts of private organizations that may otherwise be hesitant to collaborate because of competitive issues, limited resources or legal constraints. A coordinated and collaborative ISAO R&D program could provide a crowd-sourced model in order to reduce the cost of research and produce tangible results for the entire community. The innovations that emerge from an open source community working together to solve the cyber problems could provide exponential gains in improving our total cyber posture.

ISAO R&D Leadership

There has been a history of obstacles in coordinating and collaborating research and development efforts among multiple diverse organizations. A lack of clear leadership to create the R&D goals and strategies is often a challenge. Frequently regulatory and legal barriers prevent open cooperation. In circumstances where multi-sector organizations have come together, the diverse economic drivers often leaves unbalanced stakes and prevents long sustained success.

ISAOs serving as champions of R&D programs can provide a unified approach and overcome many legacy R&D obstacles. ISAO communities will assemble based on common organizational attributes such as market, region or sector. Their assemblages will align a community of organizations with common emerging threats, R&D appetites and relationships to markets.

In order to make the best use of the assembled organizations and resources all focused on cyber security, ICF urges the ISAOs take the initiative in leading the development of R&D programs in these specific areas.

- Establish an R&D program framework which balances results based objectives while permitting flexibility of commercial based endeavors.
- Promote rewarding R&D projects which are focused and compliment the program objectives of other ISAO communities.
- Lead the scoping and prioritization of R&D projects.

- Assess investment strategies and investment organizations that may help propel successful project results into production or commercial uses.
- Accelerate solution deployments by establishing roadmaps and procedures to shepherd successful projects to their end-state.
- Establish common testing environments to ensure the proposed solutions meet expectations of the ISAO community.

Strategy

Any successful research and development program requires consistent vision, guided practices, multi-year strategic objectives. There will be many players, strong desire for solutions and limited resources in the ISAO venue. In order to produce worthwhile research and developments there should exist some mechanism to guide the evaluation of R&D opportunities, determine R&D goals, develop strategic R&D plans and guide the overall R&D programs.

ISAO should assemble a R&D committee of thought leaders within their ISAO communities to lead R&D activities. This committee should develop strategic research and development objectives which align with the ISAO long term threat and risk problems. ISAOs should lead and guide R&D activities, monitor resources, and ensure the most compelling solution gaps are being confronted. ISAOs should formulate research strategies that align with their ISAO community member's common missions and needs. ISAOs should coordinate activities across a broad multi-organizational populous to produce repeatable and demonstrable experimentation results.

ISAOs should establish transition plans and pathways to steward successful prototypes and concepts to the appropriate conclusion, be that single-instance production, information sharing or for-profit markets.

ISAO R&D program leaders should create an architecture by which challenges, problems, responsibilities and resources are allocated appropriately.

ISAO should establish partnerships with law firms specializing in cybersecurity, to identify and address common cybersecurity legal and policy concerns. These relationships could prove valuable in creating ISAO membership agreements, setting up rules of engagements for multi-organizational collaborations, promoting R&D developments to commercial markets, and establishing liability protection from voluntary information sharing.

In the event a successful and marketable solution is developed, ISAO R&D committees will lead efforts to establish rules for profit sharing, investment and costs.

Specifically, ISAOs should convene their cybersecurity leaders and key ISAO community members to develop means to:

- Establish relationships with venture capital organizations and provide conduits to investment resources that can assist in funding the development of prototypes and concepts for promotion to appropriate commercial markets.

- Evaluate, and assess the resources of the ISAO membership community to establish facilities where experts can coordinate and test threat scenarios and defense hypothesis in a safe environment.
- Address legal obstacles in transitioning prototypes and models into market solutions.
- Establish key partnerships with other industry, educational and government sector organizations to collaborate and share information, ideas, and strategies.
- Maintain awareness of parallel market development and existing solutions that could offer benefits to their ISAO community members.
- Establish multi-ISAO working group to allow related R&D projects to collaborate for mutual benefit to eliminate resource duplication.
- Engage academic and other research communities to maximize opportunities to collaborate and exchange ideas about underlying vulnerabilities with other ISAO sectors.
- Solicit talent, experience and facilities from their member organizations to make efficient use of resources and channel expertise and resources from this broad community to common R&D programs.
- Leverage community membership resources and relationships to establish collaboration facilities as well as labs for testing and experimentation.

Protecting information systems and data has never been more challenging. ICF understand this is not just a big-business or critical infrastructure problem. The internet has linked every public and private organization in a codependence of interests. We can no longer silo our protection strategies. ICF is grateful for the opportunity to provide thoughts to DHS and ISAO stakeholders. We look forward to the opportunity to expand on these thoughts as well as other topics we were unable to present in this forum. In the meantime we invite your feedback and questions.

References

[i] U. S. C. E. R. Team, "Traffic Light Protocol (TLP) Matrix and Frequently Asked Questions," United States Computer Emergency Readiness Team, [Online]. Available: https://www.us-cert.gov/tlp. [Accessed 8 July 2015].