REN-ISAC Charter

Version 2.1 (July 2013)

Contents

1.0 Introduction

1.1 Sharing experiences, practices, and responses amongst organizations has long been known to improve operations in those individual organizations, and in those communities. It is no different in the world of operational security. Indeed, Presidential Decision Directive 63 (PDD 63, May of 1998) initially encouraged, and then the superseding Homeland Security Presidential Directive 7 (HSPD-7, December 2003) also encouraged the sharing of security information amongst various sectors of the economy, and encouraged the creation of "sector information sharing and analysis centers (ISACs)". The Directive recognized that various sectors of the economy experience security (physical and logical) events and threats at varying intensities and points in time. Sharing incident information with other sectors may provide the impacted/reporting sector with ideas for minimizing impact and recovering from the event; it would also likely allow for planning and implementation of mitigation techniques in sectors to which the threat has not yet reached. Clearly, increasing the scope of sharing results in greater security preparedness for all involved.

1.2 HSPD-7 discusses coordination with the private sector:
In accordance with applicable laws or regulations, the Department and the Sector-Specific Agencies will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms. Additionally, the Department and Sector-Specific Agencies shall collaborate with the private sector and continue to support sector-coordinating mechanisms to:

(a) Identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and

(b) Facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.

2.0 History

2.1 The National Infrastructure Protection Center (NIPC, then part of the FBI, but since subsumed by the Department of Homeland Security) was tasked by PDD 63 to coordinate the sharing centers that would represent various sectors (e.g., Transportation, Food, Energy, Telecommunications, Information Technology, etc.). Several people involved in security at Indiana University saw that Higher Education was NOT represented in the initial structure of sectors being described by the NIPC, and so would not participate in (or benefit from) this sharing scheme. Then-Indiana University Vice President and Chief Information Officer Michael McRobbie met with Admiral James Plehal, then-Director of the NIPC, and discussed the situation. Subsequent interactions between Indiana University, EDUCAUSE, and Internet2, with Richard Clarke and others in US government lead to discussions of developing higher education representation. Concurrently, EDUCAUSE and Internet2 both identified a formal sharing mechanism an important component of the higher education security approach.

2.2 Indiana University has invested greatly in the areas of "information and infrastructure assurance." In addition, as operator of the Global Research Network Operations Center (GR-NOC), Indiana University has a unique view of various national and international R&E networks, including Internet2 and National Lambda Rail (NLR). Because of these network relationships, Indiana University necessarily has some of the best network engineers in the US. The Service Desk of the GR-NOC monitors

the networks for which Indiana University has management responsibility 24x7, including network instrumentation and other sources of specific information about security events.

2.3 Indiana University was a charter member of the EDUCAUSE & Internet2 Computer and Network Security Task Force [5].

2.4 It was due to these competencies, relationships, and functions, along with a desire on the part of Indiana University to improve security locally and in the higher education community, that the first ISAC serving higher education - the Research and Education Networking ISAC (REN-ISAC) - is based at Indiana University. Hosting the REN-ISAC (as a participant in the national ISAC structure) at Indiana University was formalized in D.C. on February 21, 2003.

2.5 Subsequently, the REN-ISAC was identified as a component of an emphasis on operational security by, and as an enhancement of security services already provided by Indiana University to the Internet2 community. EDUCAUSE has identified the REN-ISAC as a primary component of the joint EDUCAUSE/Internet2 effort to improve security across higher education. The REN-ISAC will, where possible and feasible, work in conjunction with these efforts to further the general goals of improving security across the higher education community.

3.0 Membership

3.1 The REN-ISAC serves colleges and universities, teaching hospitals, research and education network providers, and government-funded research organization. Institutions are members, and one or more individuals who satisfy a set of criteria represent each member organization.

3.2 Membership details can be found in the Membership Guide [6].

3.3 Other general terms and conditions of REN-ISAC membership and operations can be found in the Membership Terms and Conditions [7].

4.0 Mission

4.1 The REN-ISAC mission is to aid and promote cybersecurity operational protection and response within the research and higher education (R&E) communities. The mission is conducted through private information sharing within a community of trusted representatives at member organizations, and as a computer security incident response team (CSIRT) supporting the R&E community at-large. REN-ISAC serves as R&E's trusted partner in commercial, governmental and private information sharing relationships, in the formal U.S. ISAC community, and for served networks.

5.0 Reporting, Sharing, and Projects

5.1 The REN-ISAC provides information products and services, and engages activities toward satisfying the Mission. A description of the products, services, and activities can be found at the REN-ISAC web pages [1]. Some examples follow.

1. The REN-ISAC distributes a daily situational awareness report based on observations from sensors and instrumentation, member input, information gathered from information sharing relationships, and open sources.
2. The REN-ISAC sends notifications to campuses affected by security incidents, aiding those campuses to immediately identify and stop the activity, and recover and repair affected systems. Depending on the severity of an incident and sources of information, notifications may occur in real-time, or in daily bulk distribution of incident notifications. Further, the information may be sanitized and shared to member campuses, other ISACs, and trusted information sharing partners, when the information could help others respond to widespread attacks, improve local security posture, and/or avoid future impact.
3. The REN-ISAC distributes bulk information (IP addresses, DNS names, URLs) regarding known bad actors, so that members can protect their networks and systems, and identify compromised machines in their domain.
4. The REN-ISAC provides channels for members to communicate and share information in a private and trusted setting.
5. The REN-ISAC receives and analyzes reports from members regarding systems that are the source or victim of a network attack, or are being seriously degraded due to unknown and suspicious cause.
6. REN-ISAC responds to requests for information and analysis from members, government agencies, and other sector ISACs.

5.2 All sharing is dictated by the policies and statements described in the Information Sharing Policy[2].

6.0 Leadership

6.1 Staffed leadership includes an Executive Director and a Technical Director.
6.2 The Executive Advisory Group, Technical Advisory Group, and Membership Committee provide consultation to the REN-ISAC directors (see Community Input and Advisory below).

7.0 Sustainability

7.1 General

7.1.1 Resources must keep pace with growth resulting in a sustained high level of benefit to members.

7.1.2 Membership fees are established as a function of the total cost of operations (based on membership desires and needs) and the number of members at a given time. Fees are set to only what is necessary to cover the costs of functional and beneficial services. (That is, the REN-ISAC will not become a for-profit entity.)

7.1.3 REN-ISAC staffing fluctuates as a function of the needs of the membership.

7.1.4 Additional participation by individual members (direct involvement in advisory or technical groups, in developing and providing services, or in active participation in discussions and in providing useful intelligence information) has and will continue to be critical.
7.1.5 While seeking funding is not a major component of staff activities, the REN-ISAC staff will be watchful of sponsorships and other appropriate tangible support opportunities.

7.2 Agency

7.2.1 Given that Indiana University (an agency of the State of Indiana), is the administrative and fiscal agent of the REN-ISAC, financial operations of the organization will adhere to Indiana University fiscal policies [8].
7.2.2 With that caveat, to the extent possible and allowed, the REN-ISAC staff will seek input and advice from sitting advisory groups as representatives of the membership, and under certain circumstances directly from the membership, on financial aspect of operations.

7.3 Basic Financial Principle

7.3.1 REN-ISAC will not be operated to generate and disseminate profit, but also cannot be a cost center of any particular sponsoring or supporting organization.
7.3.2 The fundamental financial goal of the REN-ISAC is to cover all costs through a combination of tangible sponsorship, support, or other philanthropic revenue and fees, and given the expense parameters and the fiscal environment in which the REN-ISAC operates.

7.4 Costs

7.4.1 Operational expenses incurred will be reasonable and necessary to support the goals of the organization. Expenses will be managed by the REN-ISAC Executive Director, in consultation with the Executive Advisory Group.
7.4.2 These costs include:

1. All applicable expenses, including but not limited to labor, travel, supplies and materials, services, maintenance, utilities, fixed charges and rentals, capital outlays and related charges, and management and administrative fees;
2. Retention for reserves to provide working capital, replacement of facilities and equipment;
3. Other expenses normal to orderly administration and operation of an information and technology-oriented activity, including mitigation of impact of disruptions to service (e.g., business continuity and disaster recovery) and physical and logical security.

7.5 Relationships

7.5.1 All interactions between the REN-ISAC and other agencies must directly support the fundamental goals of the organization.
7.5.2 Any proposed relationship (involving tangible sponsorship, information sharing, or similar considerations) between the REN-ISAC and other organizations (especially commercial entities) will be discussed with the Executive Advisory Group and the Technical Advisory Group, which will provide advice as to how/whether to proceed.

7.6 Membership Fees

7.6.1 Members will be charged an annual rate consistent with the cost statements above.
7.6.2 Rates are set annually, at the decision of the Executive Director, in consultation with the Executive Advisory Group.

7.6.3 Nominal increases may be applied to offset staff cost-of-living, inflationary, and other nominal increases in expenses.
7.6.4 Less frequent larger changes in rates may be necessary to cover costs incurred by improvements in operations and services provided.
7.6.5 Fees are published in the Membership Fees document [3].

7.7 Reserves

7.7.1 Excess reserves, as determined by REN-ISAC staff, in consultation with the Executive Advisory Group, will be used to offset increases (and potentially allow for decreases) in membership fees.

7.8 Reporting

7.8.1 REN-ISAC staff will provide an annual budget and expense summary report to the members within one month of fiscal year close. At the request of the Executive Advisory Group Chair, a detailed budget and expense report will be provided to the Executive Advisory Group.

8.0 Community Input and Advisory

8.1 General

8.1.1 Executive and technical advisory groups, and the membership committee, are assembled from the membership, and they represent the membership. They assist REN-ISAC staff in navigating policy issues, refining and developing information products and other services, and ensuring viable membership procedures and processes. Membership of the groups is by invitation, and will be representative of the U.S. higher education demographics.
8.1.2 Other committees and groups will be formed as necessary to support the goals of the REN-ISAC and of the membership.
8.1.3 Current membership and other information about community advisory can be found at the Advisory Groups web page[4].

8.2 Executive Advisory Group (EAG)

8.2.1 The Executive Advisory Group (EAG) advises REN-ISAC directors regarding policies, legal issues, plans and strategies, and other non-technical aspects of REN-ISAC operations.
8.2.2 The EAG is composed of approximately five to seven members and one or more liaisons appointed by the REN-ISAC Executive Director. EAG members will be individuals who are broadly versed in information technology legal, policy, and general security issues and concerns. Not more than one sitting EAG member will be from an individual organization. Chief Information or Technology Officers, university lawyers, and senior IT policy security officers are likely candidates.
8.2.3 The chair of the Technical Advisory Group (below) is a member of the EAG.
8.2.4 Other aspects of the EAG are described at the Advisory Groups web page[4].

8.3 Technical Advisory Group (TAG)

8.3.1 The Technical Advisory Group (TAG) advises the REN-ISAC technical staff regarding information products, services, and methods, threat intelligence, and other technical aspects of REN-ISAC operations.

8.3.2 The TAG is composed of approximately ten individuals and one or more liaisons appointed by the REN-ISAC Technical Director. A super majority of the TAG is drawn from the REN-ISAC membership. Individuals drawn from outside REN-ISAC membership are vetted by the TAG and given XSec member status during their appointment.

8.3.3 Other than as published in reports to the membership, information provided to the TAG and its deliberations are private.

8.3.4 Other aspects of the TAG are described at the Advisory Groups web page[4].

8.4 Membership Committee

8.4.1 The Membership Committee monitors the member application process, including the vouching for prospective member representatives. It responds to applicant and member questions and concerns. It judges cases of dissent regarding prospective member representatives, reproach of current member representatives, and makes recommendations to the REN-ISAC directors regarding appropriate response. In addition, the Committee supports member awareness of REN-ISAC policies, and monitors compliance; identifies and makes recommendations regarding member and prospective member needs and perceptions; recommends ways to increase REN-ISAC membership, especially among underrepresented segments of the U.S. research and education community; recommends ways to make prospective and current members aware of the resources, services, and benefits of REN-ISAC; welcomes new members and encourages participation in REN-ISAC activities; and in cooperation with REN-ISAC directors and the Executive Advisory Group, adjudicates cases of policy breach.

8.4.2 The Membership Committee is composed of appointed members and the REN-ISAC Technical Director. Appointments are made by the Executive Director. The Committee chair responds to requests from the Executive Advisory Group, and works with the chair of the EAG on cases of member discipline. The Committee submits annual reports to the Technical Director in advance of the REN-ISAC Annual Member Meeting.

8.4.3 Other mechanics of Membership Committee operation are described at the member-private Advisory Groups web page.

Footnotes

REN-ISAC; http://www.ren-isac.net

Information Sharing Policy; http://www.ren-isac.net/docs/information_sharing_policy.html

Membership Fees; http://www.ren-isac.net/docs/fees.html

REN-ISAC Advisory Groups and Analysis Teams; http://www.ren-isac.net/about/advisory.html

EDUCAUSE & Internet2 Computer and Network Security Task Force; http://www.educause.edu/security

Membership Guide; http://www.ren-isac.net/docs/membership.html

Membership Terms and Conditions; http://www.ren-isac.net/terms_and_conditions.html

Indiana University Financial Affairs - Policies; http://www.indiana.edu/~vpcfo/policies/