SIRTFI: Key to Managing Federation-Related Security Incidents

InCommon and REN-ISAC, alongside international partners, strongly urge federation participants to be ready to manage federation-related security incidents. Here's how.

SIRTFI is an international framework for federated security incident response. It specifies a means to publish your readiness for incident response in federation metadata. This framework asks that each federation entity, ie, Identity and Service Providers, contain security contact information in its federation metadata; that normal security incident response procedures associated with it reasonably address the statements in the SIRTFI specification; and if so, that a SIRTFI tag is attached to the entity.

InCommon recently made self-management of the security contact and SIRTFI flag available in its Federation Manager portal. Participant Site Administrators can now manage SIRTFI status for all systems that are part of the Federation. Please ask them to ensure that your security contact information is correctly expressed in federation metadata and to set the SIRTFI flag if you believe that your security incident response procedures reasonably meet the statements in the SIRTFI specification. Step-by-step instructions are here.

Academic collaborations, cloud services, and other uses depend on sensitive resources, such as unique instruments, software, high performance data processing environments, and corpi of data, being accessible through global federation. Most InCommon participants are home to faculty, students, and staff that need to use these services to be successful in their endeavors. Please help them to succeed by being prepared to manage a federated security incident that could otherwise threaten valuable resources.

Kim Milford
Executive Director, REN-ISAC
Member, InCommon Technical Advisory Committee

Kevin Morooney
Vice President Trust & Identity Services, Internet2