Security Contacts in SAML Metadata

Jim Basney
jbasney@ncsa.illinois.edu
Topics

• About InCommon
• Federated security incident response
• Security contacts in metadata
  – Metadata integrity
  – Examples and statistics
  – Open questions
## Federation Info: Organizations

<table>
<thead>
<tr>
<th>Organization Name</th>
<th># of IdPs</th>
<th># of SPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carnegie Mellon University</td>
<td>2</td>
<td>421</td>
</tr>
<tr>
<td>Symantec Corporation</td>
<td>1</td>
<td>229</td>
</tr>
<tr>
<td>Quattros Labs, Inc.</td>
<td>0</td>
<td>162</td>
</tr>
<tr>
<td>Academic Works, Inc.</td>
<td>0</td>
<td>128</td>
</tr>
<tr>
<td>University of Chicago</td>
<td>1</td>
<td>99</td>
</tr>
<tr>
<td>PeopleAdmin, Inc.</td>
<td>0</td>
<td>81</td>
</tr>
<tr>
<td>University of Washington</td>
<td>1</td>
<td>68</td>
</tr>
<tr>
<td>Terr Dotts, LLC</td>
<td>0</td>
<td>59</td>
</tr>
<tr>
<td>University of California - Office of the President</td>
<td>1</td>
<td>47</td>
</tr>
<tr>
<td>Atlas Systems, Inc.</td>
<td>0</td>
<td>45</td>
</tr>
<tr>
<td>Cusago, Inc.</td>
<td>0</td>
<td>42</td>
</tr>
<tr>
<td>University of California-Los Angeles</td>
<td>1</td>
<td>43</td>
</tr>
<tr>
<td>UniversityTickets</td>
<td>0</td>
<td>37</td>
</tr>
<tr>
<td>Penn State</td>
<td>1</td>
<td>33</td>
</tr>
<tr>
<td>MCNC</td>
<td>1</td>
<td>33</td>
</tr>
<tr>
<td>Instruction, Inc.</td>
<td>0</td>
<td>31</td>
</tr>
<tr>
<td>Internet2</td>
<td>1</td>
<td>30</td>
</tr>
<tr>
<td>Edublogs</td>
<td>0</td>
<td>26</td>
</tr>
<tr>
<td>Ex Libris North America</td>
<td>0</td>
<td>25</td>
</tr>
<tr>
<td>Imodules Software, Inc.</td>
<td>0</td>
<td>25</td>
</tr>
<tr>
<td>HighWire Press</td>
<td>0</td>
<td>23</td>
</tr>
<tr>
<td>Indiana University</td>
<td>1</td>
<td>21</td>
</tr>
<tr>
<td>University of Maryland College Park</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td>California State University, Office of the Chancellor</td>
<td>1</td>
<td>16</td>
</tr>
<tr>
<td>Northwestern University</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>Desire2Learn Inc.</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>eLearning Solutions, LLC</td>
<td>0</td>
<td>15</td>
</tr>
</tbody>
</table>

### Summary Statistics
- Total # of Orgs: 577
- Total # of IdPs: 414
- Total # of SPs: 2578

### Higher Education Participants (525)
- A.T. Still University
- Adventist University of Health Sciences
- Aims Community College
- Allan Hancock Joint Community College District
- Allegheny College
- American Public University System
- American University
- American University of Beirut
- American University of Sharjah
- Amherst College
- Antelope Valley Community College District
- Arizona State University
- Arkansas State University
- Auburn University
- Augustsburg College
- Arizona Pacific University
- Ball State University
- Baltimore City Community College
- Barry University
- Bates College
- Bay De Noc Community College
- Baylor College of Medicine
- Baylor University
- Beaufort County Community College
- Berklee College of Music
- Binghamton University
- Blackburn Technical College
- Blinn College
- Bloomsburg University of Pennsylvania
- Bob Jones University
- Boise State University
- Boston College
- Boston University
- Bowdoin College
- Bowling Green State University
- Brandeis University

### Government and Nonprofit Laboratories, Research Centers, and Agencies (33)
- Ames Laboratory
- Argonne National Laboratory
- Brookhaven National Laboratory
- BSN
- BSX - Stanford Linear Accelerator Center (SLAC)
- Fermilab
- GENI Project Office
- Idaho National Laboratory
- Internet2
- Jefferson Lab
- Lawrence Berkeley National Laboratory
- Lawrence Livermore National Security, LLC/Lawrence Livermore National Laboratory
- LSUQ Scientific Collaboration
- LTER (Long Term Ecological Research Network)
- Marine Biological Laboratory
- National Institutes of Health
- National Science Foundation
- NERSC (National Energy Scientific Computing Center)
- Oak Ridge National Laboratory
- Open Cloud Consortium (OCC)
- Open Science Grid
- Pacific Northwest National Laboratory
- Sandia National Labs
- Smithsonian Institution
- The Broad Institute of MIT and Harvard
- The FDP Foundation
- The MITRE Corporation
- The Translational Genomics Research Institute
- The University Corporation for Atmospheric Research
- U.S. Department of Energy Office of Scientific and Technical Information (OSTI)
- United States General Services Administration

### Sponsored Partners (238)
- 12Twenty Inc.
- Astra USA
- Academic Works, Inc.
- Acator
- Accessible Information Management, LLC
- Active Network
- Adobe Systems, Inc.
- Advantage Connect Pro Inc.
- AEFIS
- ALEGIS Corporation
- Alexander Street Press
- AliveTek
- American Medical Association
- Applied Training Systems, Inc. dB/a dBReview
- Apple
- AppleInc Portal Solutions, Inc.
- ARToolKit
- Association for Computing Machinery
- AT&T Services
- AthenaOnline.com
- Atlas Systems, Inc.
- Atomic Learning
- Axiom Education
- BeneLogic
- BioOne, Inc.
- BioRAFT
- Blackboard, Inc.
- Blatant Media Corporation
- Blue Jeans Network
- BoardShift
- Box, Inc.
- C.A. Short Company
- Cambridge University Press
- Campus Quad
- Campus Technologies
- CampusGuard

---

**InCommon**

**Federation**

**Federation Info:**

**About** | **Organizations** | **Entities**

---

**InCommon**

**Current InCommon Participants**

Below is a complete list of InCommon Participants. There are also lists available for:

- Identity and Service Providers deployed in the federation (and other metadata-driven pages)
- Certificate Service subscribers
- Duo Security multifactor service subscribers

The IdP and SP pages include links to more-detailed information on each entry—just go to the IdP or SP list and click on the name of the IdP or SP you are interested in.

**InCommon serves 8 million end-users through federated identity management (PESI data; October 2014)**
Federated Security IR

- InCommon Recommended Practice:
  - https://spaces.internet2.edu/x/8o6KAQ
- **Publish IR contact information in metadata**
- Implement a log retention policy for identity providers and service providers
- Document procedure for responding to a federated security incident
- See also: https://wiki.refeds.org/display/GROUPS/SIRTFI
SAML Metadata

• Published by federation operators
• Digitally signed
• Contains entity names, endpoint URLs, public keys, and contact info
  – Vetted by federation operators via documented registration process
• InCommon example: https://spaces.internet2.edu/x/xodHBQ
InCommon Example

<EntityDescriptor entityId="https://cilogon.org/shibboleth" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      </ds:KeyInfo>
    </md:KeyDescriptor>
  </SPSSODescriptor>
  <Organization>
    <OrganizationName>University of Illinois at Urbana-Champaign</OrganizationName>
    <OrganizationURL>http://illinois.edu/</OrganizationURL>
  </Organization>
</EntityDescriptor>
Contacts in Metadata

• **technical contact**: for direct communication between InCommon participants regarding technical issues such as troubleshooting software, systems, or networking issues

• **support contact**: for end-user technical support but may also handle questions from users regarding attribute release policy, user privacy, or access issues relating to assurance

• **administrative contact**: for direct communication between InCommon participants and by institutional users regarding non-technical issues such as attribute release policy, on-boarding issues, privacy, or assurance certification

• **security contact**: for direct communication between InCommon participants regarding security matters, especially for the purposes of Federated Security Incident Response

• https://spaces.internet2.edu/x/BomKAQ
Proposed REFEDS Definition

Security contact information is for direct communication between organizations operating within the context of identity federations, to facilitate coordination of response to an information system security incident. The expectations of those contacted are described in the Sirtfi Trust Framework.
InCommon Metadata Statistics

122 unique security contact email addresses
99 out of 577 (17%) orgs w/ sec contacts
72 out of 414 (17%) IdPs w/ sec contacts
138 out of 2578 (5%) SPs w/ sec contacts
210 out of 2992 (7%) entities w/ sec contacts
Open Questions

- What should security contact in metadata contain?
  - EmailAddress, GivenName, TelephoneNumber, and/or URL (for PGP key fingerprints)?
- May contain contact info for department, institution, or NREN CERT?
- How “trusted” is the security contact?
- What are the expectations on response?
- Fall back to “technical contact” if no security contact provided?
- Use for only IdP/SP incidents or more general account (identity) management or endpoint security incident?
- Sufficient value to promote security contact registration across federations?
Thanks!

jbasney@ncsa.illinois.edu