DRAFT - InCommon Strategic Priorities

January 23, 2014

Developed by the TAC and delivered to InCommon Steering

Summary

InCommon Steering recently asked its Technical Advisory Committee (TAC) to develop a set of recommendations for a multi-year program, staffing recommendations, immediate priorities, and thoughts on organization of committees to support that work. This paper is a first response to that request. We offer some thoughts on some of the immediate issues that should be addressed, and have identified a list of Technical Priorities that we feel should be addressed first. More broadly, though, we have used "The Seven InCommon Steering Strategic Priorities" developed during the November 2013 Face-to-Face in San Francisco as an organizing framework, and have laid out a broader multi-year program of services and changes that can strengthen and deepen the InCommon Value Proposition, and provide a broader set of common shared services and value to members. InCommon is only as strong as the engagement and participation of its members; these proposals aim to strengthen those connections.

We have provided a list of Calendar 2014 Priorities. However, within the multi-year program, we have not yet made any attempt to prioritize or sequence the various recommendations, or associate resource estimates with specific items. We think it is too early in the discussion to explore those issues; in any case, we did not have time to think through the resourcing questions. We view submitting this document as the start of a discussion with Steering and its Programs Subcommittee, the beginning of a process. We expect that the contents of this document will evolve over time, and that the discussion will expand to cover timeline, resources, and associated metrics. All of the 2014 recommendations are new items; all of these are significant efforts, requiring assigned resources. However, it is very clear that serious efforts to address the recommendations in this document will require additional staffing or shifts in responsibilities at InCommon.

In addition, there has been little discussion to date about how best to organize ourselves, the future role of the TAC, or whether the organization of the TAC should change (or not) to support these priorities. That, of course, will depend on the actual decisions that are made about 2014 Programs. This document mentions several new committees. However, as noted, there has been little discussion to date about how to organize these groups and how they would communicate with each other. Many of the recommendations in this document extend the Role of InCommon. However there has been no discussion as of yet about how the membership of the TAC might or should evolve in order to better address some of the new Priorities.

Lastly, some of the recommendations in the “Key Values and Themes” section of this document go beyond the traditional scope of the TAC. They often refer to InCommon, and may seem to imply that InCommon has not done enough in the past. That is not the intent. InCommon is “us”. We are the ones that make decisions, and make things happen. InCommon is at an inflection point, and can decide which path to pursue in the future. These recommendations are an effort to help define one of the possible paths forward.

Calendar 2014 Priorities

1. Know who we are and tell others
    1.1. Define the scope of InCommon
    1.2. Develop and disseminate the InCommon value proposition
    1.3. Develop a community engagement plan for collaborating with participants more broadly and more effectively for purposes of gathering requirements, planning, setting priorities and promulgating new practices to enhance trust
2. Make federation easy to deploy
    2.1. Provide to campuses a package for a mature operational Shibboleth IdP, including support for the optional use of MFA.
3. Demonstrate commitment to the needs of the Research community by:
    3.1. Create a research support group, and hire a full-time support person who is familiar with the needs of this community
    3.2. Working directly or with partners, deploy a Research Community IdP with ECP capability for R&S SPs
    3.3. Complete deployment of InCommon IGTF Server CA for XSEDE.
4. Create an IAM Directions group to support CIOs in their efforts to advance IAM functionality on their campuses by defining a strategic roadmap and providing technology solutions.
5. Integrate with the larger fabric
    5.1. Extend the reach by implementing the interfederation subcommittee recommendations (both internationally and with US K12).
    5.2. Broaden access by facilitating the availability to all member SPs of a lightweight Social-SAML gateway.
6. Work with the community to identify real Assurance needs, and develop a Higher Education Assurance profile to address those needs.
7. Continue Advance CAMP, a community forum for identifying and making progress on community identity-related issues

Key Values and Themes

Define the Service Scope of InCommon. From the outset, InCommon has defined itself with a much narrower service profile to its members than most other Higher Education Federations around the world. InCommon, for instance, offers no real support to its members. This was intentional, and was consistent with the initial funding and membership models used by InCommon. But, InCommon has grown from 20 to nearly 500 member campuses. In addition, many of the other national Higher Education Federations directly provide services to their members to support their use of Federation, rather than asking members to contract in the marketplace for generic services. It is a different environment, and it may be time for a different model.

Communicate the InCommon Value Proposition. There does not exist a clear, concise, value-laden, published statement conveying InCommon's Value Proposition. Many of us are asked this question, and we all have different answers. We all understand how having a common shared purpose and goals helps to align our activities and to "sell" the Federation. We all work at campuses that are able to state their Value Proposition; InCommon needs to be able to do the same. InCommon is the shared infrastructure shared national education and research goals.

Expand InCommon from Federated Identity to a Broader Definition of Identity. Steering has recently moved to redefine InCommon as “Trusted Identity in Education and Research” (TIER). This step recognizes the strong dependence of Federated Identity on effective campus IAM practices. Yet many campuses find themselves unable to muster the resources and expertise needed to create that central IAM service. Even at campuses with greater skills and resources, CIO’s regularly ask for help in developing approaches to their campus IAM problems. They ask for roadmaps, best practice information, case studies, short term consulting, and software. Significant campus preparation is required in order to participate effectively in the Federation; the path and phases need to be described. InCommon should aim to become the authoritative source for these needs.

Engage with the Community. InCommon defines itself as being "for and of the members". However, there is very little communication in either direction. There must also be engagement with the next round of InCommon members, educating them to the value proposition and learning their needs.

Make It Easily Deployable. InCommon expects its members to install and operate complex software in order to gain value. This is beyond the skills and resources available to many of the new and potential members. The Affiliate Program offers some help; however, InCommon itself offers essentially no support to new members, or even a welcoming email pointing to resources. There is not even a Help Desk. These potential members install and run (with help) commercial ERP systems; their path to InCommon might be easier if these systems included the Federating software.

Integrate with the Larger Fabric. The Fabric has grown in recent years. It now includes Higher Education/Research Federations around the globe, a growing array of standards and user support groups, and increasing participation from the K12 space. Many of the ideas, practices, and standards that allow interoperation were developed years ago by working groups sponsored by the Internet2/MACE group. In recent years, though, invention is increasingly happening elsewhere. Full and effective participation by US R&E IAM leaders in new arenas such as REFEDS, ISOC, and eduGAIN is needed.

Support the Research Community. The Internet has spurred the growth of research groups that draw their memberships from multiple campuses. InCommon should do more to help these communities gain value from leveraging the Federation. Too many times big funded research groups look at InCommon and walk away, saying its not enough of a solution to justify the work required to become compatible. The research community needs service offerings that meet their needs and a liaison to ensure continuing alignment and effectiveness.

InCommon Needs to Mature its Infrastructure. InCommon is the largest Higher Ed/Research Federation in the world. The continuing growth in membership requires that inCommon mature its infrastructure, scaling it up, hardening it, and instrumenting it. We need to think about the

implications of continued growth, while maintaining the simplicity of operating within the Federation that we have worked so hard to achieve.

Communicate the InCommon Privacy Story. There is no need to revisit the litany of news stories since last summer about privacy violations via public and private networks. One of InCommon's primary differentiators, though, is sending PII over the networks. We need a coherent understandable story about what InCommon does to help protect personal privacy.

Measure Progress. InCommon needs to develop a framework to measure its progress. Many of us already familiar with this strategy, and use it on our campuses. InCommon needs to regularly identify a set of Critical Success Factors, and measure its progress against them.

All of This Will Take Resources. Achieving our goals will take a lot of work. The tasks described here represent new work added to the important work already done by InCommon's staff and the volunteers who comprise the membership of InCommon's Steering Committee, the Technical Advisory Committee, the Assurance Advisory Committee, and the multiple work groups that address today's issues. The issues addressed by this document will require greater investment, particularly for staff.

In addition, much IAM expertise resides at the campus level and this community has demonstrated its ability to develop the practices that enable our current level of interop. Funded partial release time has contributed to that outcome. As one component of a resourcing strategy, and as one means of incenting the growth of "seed corn", we advocate continued use of this approach.

The Seven InCommon Steering Strategic Priorities

1) Making It Easier to Federate IdPs and SPs

- o Social 2 SAML
- o Community specific IdP(s)
- o "Federation Ready": Easy deploy installers, guides, config mgrs

InCommon Service Desk

1. provide Tier 1 support to participants deploying IdP and SP software
2. work with the shibboleth project to identify common issues and their resolutions
3. ditto simpleSAMLphp, Microsoft, others as deployment widens
4. document requirements and recommended practices specifically for Sponsored Partners
5. provide 24/7 operational support for InCommon certificate service (certificate revocation, responding to OCSP service outages, expediting critical certificate issuance, etc.)

Simplify the Process for Deploying and Managing an IdP and SP in the Federation

1. Provide guides, configuration managers, and templates to help sites evolve their IdPs and SPs to become “Federation ready”, rather than just a minimal deploy
2. InCommon should provide a simplified process (and perhaps a platform) for applications to become active SPs within the Federation (perhaps with limited SP functionality; see UK, Canada, Australia REFEDS slides - https://refeds.org/meetings/nov13/)
3. Devise a strategy for Active Directory and AD FS. The question of interoperability with AD FS was a popular topic during the Steering Committee’s recent webinar. This will allow for the multitude of “Microsoft only” shops to more readily join the Federation.
4. Usability: Federating software like Shibboleth and simpleSAMLphp are too complex to install and configure. GUI mechanisms are needed to simplify the configuration for SPs and then IdPs. The GUI should also link back to documentation available online. A group needs to investigate tools and practices to make this much easier.
5. Approach the ERP and other vendors about including Shibboleth support in their products. One problem is that Shibboleth is moving further and further away from a straight SAML2 implementation, to including niceties like metadata parsing for entity tags that we need and other products do not have. Leif Johansson’s ADFS work is one really important activity. We need a plan for how to engage these companies.

Managed IdP Service: Federating Organizations & Last Resort for Individuals

Operate or contract a managed IdP service that enables a wider range of campuses to participate by reducing their technical barriers and providing a range of valuable capabilities, and by providing an IdP of Last Resort for individuals lacking other options.

1. SSO backended by existing campus authentication service and attribute sources
2. 2nd factor add-on located at managed IdP service reduces barrier to adopting stronger authentication

    2.1. option to link with campus registration/onboarding personnel to support higher LoA
3. “InCommon guest” accounts for those having no affiliation with an IdP Participant
4. Linking of social IDs to support online learning and other loosely affiliated use cases
5. Entity category support
6. Integrated user consent
7. ECP support

This service can be one means by which some of the components that follow are implemented.

A Social-to-SAML Gateway

Campuses increasingly see value in leveraging the Social IDs that so many of their members and others already have. Use cases range from alternatives to campus “guest accounts” for specific and limited purposes to replacement of campus-issued credentials for some segments of their traditional population. This gateway provides a common technical solution so that they don’t need to reinvent one. When operated as a service managed by InCommon, this gateway further provides a means for people at US HE institutions that are not yet InCommon IdP Participants to participate in collaborative activities supported by InCommon SPs having low LoA requirements.

1. InCommon should find a way to make available a lightweight Social-to-SAML Gateway that could be used by all member SPs as part of their InCommon membership. This Gateway would provide a narrow set of services (reassert only email and person name, manufacture and assert ePPN at the Gateway, no extra attributes, no trust elevation, no invitation service)
2. InCommon might identify other ways to gain value from a Social-to-SAML Gateway (e.g., a higher tier of Social-to-SAML Gateway service for R&S SPs).
3. Individual campuses might contract for higher levels of service from a Social-to-SAML Gateway

IdP of Last Resort: Federating Individuals

The primary motivation for an IdP of Last Resort (IdPoLR) is to attract SPs supporting research projects with multi-campus membership to join InCommon. Given the current low penetration of InCommon within US higher ed (approximately 20% of US HE institutions operate InCommon IdPs), an IdP offering more than basic services is essential to provide a complete federation solution. Many SPs walk away from InCommon because its “IdP reach” is too narrow.

Research SPs, in particular, often need either or both of SAML ECP support and MFA support in the IdPs they interoperate with; the Social-to-SAML Gateway is unlikely to provide this support. While an IdPoLR requires the user to create yet another username and password, and perhaps obtain additional credentials beyond a password, the added functionality will gain them access to sites with stronger security requirements.

Simplified Integration (Identity Integration Group)

- Simplify technical interop with NET+ providers
- Work with vendors to document how to Shibboleth-enable popular apps that campuses run locally (e.g., Banner, Oracle ERP apps)
- Promulgate a vision for integrating CAS and Shibboleth (Shibboleth IdP v3)

More Education and Training.

InCommon offers Shibboleth training; it has already filled the 2014 schedule and there is already a waiting list of campus sites requesting training for 2015. Education and training are particularly important for new members Part of making it easier to federate is to help folks understand the why, how, and when.

2) Increasing Value of InCommon Participation

1. Delegated admin, other tools
2. Localized custom metadata aggregates
3. Expanding as a services organization: managed services, support
4. High-value commercial services in federation
5. Scaling, Maturing, and Hardening Federation Operations

There are two aspects to the “increasing value” statement:

- increase the value of participation to encourage additional campuses to make the “join” decision
- increase the value of participation for existing members

Increasing Value for New Members

The 80% of US Higher Education institutions that are not currently InCommon members often ask “why should I join InCommon? What Value is obtained from the one-time and ongoing effort and costs?”. Currently, none of us have a simple, straightforward, and convincing response. An answer might include:

1. simplify access and interop to high value cloud-based applications
2. simplify non-community access to local enterprise systems (eg applicants to applicant system; Continuing Ed students accessing an LMS, etc).
3. access to a community of experts sharing experiences and solutions
4. access to an array of services and hosting solutions to simplify the use of Federation

It seems likely that potential new members will use a very different value equation than the original and current InCommon members. There will be less of the “its the right thing to do” view, and a more business-like evaluation of cost, value, and risk.

InCommon has traditionally relied on its members to nominate commercial partners and bring them into the Federation. If the value equation is changing, though, then InCommon may have to

take a more proactive approach to identifying high-value commercial sites and encouraging them to join InCommon.

We also need to expand the services provided by InCommon beyond the essentials we provide today. InCommon is already taking steps in this direction with the certificate service and by providing tools to enable InCommon Federation to be used as the local federation for a campus. Should InCommon offer Federation-level external identity (social-to-SAML) services? What services beyond Federation should be offered? While technical feasibility is important in consideration of new services, business drivers and predicting where the puck will be are important aspects to service considerations going forward. This effort could also evaluate services for identity integration along the lines of what Nate does on a regular basis via NET+. TAC should be working with members of the community to help identify identity and trust-related services not yet available to our community. It is unclear if this should be a TAC-driven process.

Service Evaluation Group

Not all services are NET+ Services. There are a variety of capabilities campuses and others need for meeting the needs of identity integration and support. Evaluate the need for new services not available today and make recommendations. Evaluate existing services and recommend changes. This group might also be involved in integration efforts for NET+. It sounds like a stretch but it could make sense to evaluate services from an identity perspective. This group would also pay attention to the issues mentioned around Scaling, Maturation and Hardening.

Increasing Value for Current Members

For current InCommon members, the InCommon Federation provides a number of capabilities for which the community isn't aware. Being able to demonstrate the use of InCommon through a variety of mechanisms such as graphs and reports along with an appropriate web presence around operational statistics, may go a long way to demonstrate such value. Statistics around who is using Delegated Administration, who is using localized custom metadata and other aggregates, and who is accessing/downloading metadata are key indicators. Some of this data would be collected by central Fed Ops but Campus / vendor metrics would also have value. Such data would also help tremendously with respect to capacity planning and, in turn, staffing predictions. These statistics aren't just related to Federation operations but could also be applied to any other service like number of TLS certs issued by the Cert Service, number of orgs subscribed to a service and so on. Where possible, members should determine how best to collect and present such data.

At the campus level, such an activity is not a one-time effort but an ongoing exercise usually conducted with business partners to make sure the right data is being presented to demonstrate value. As such, demonstrating the value of InCommon should be an ongoing activity providing regular information to TAC and Steering, and then, in turn, via appropriate communications

mechanisms, to CIOs and other stakeholders. More importantly, providing information to those NOT using InCommon will likely get more organizations interested in using InCommon services.

Much of what has been mentioned thus far are operational issues but all is geared towards providing services. A graph is part of a larger service demonstrating use and value.

We also need to expand the services provided by InCommon beyond the essentials we provide today. InCommon is already taking steps in this direction with the certificate service and by providing tools to enable InCommon Federation to be used as the local federation for a campus. Should InCommon offer Federation-level external identity (social-to-SAML) services? What services beyond Federation should be offered? While technical feasibility is important in consideration of new services, business drivers and predicting where the puck will be are important aspects to service considerations going forward. This effort could also evaluate services for identity integration along the lines of what Nate does on a regular basis via NET+. TAC should be working with members of the community to help identify identity and trust-related services not yet available to our community. It is unclear if this should be a TAC-driven process.

At the recent Nov 2013 REFEDS Meeting in San Francisco other Higher Education Federations described new services they were offering to members to simplify the process of successfully participating in their Federations. It would be useful to review the presentations from Canada and Australia https://refeds.org/meetings/nov13/ Other Federations seem to be providing help to new memebrs to move them past “basic participation” in the Federation.

Lastly, but certainly not least, ensuring service scalability beyond the more traditional Internet2 top-tier institutions regarding identity and trust should be a critical consideration for any new services. We have learned over the last many years the commercial sector is not as quick as we would like picking up the needs of Higher Ed and Research so we need to be prepared to offer services for R&E, by R&E. Doing so immediately produces success and if markets develop and mature where we no longer need to offer such services then we declare success again! TAC should be identifying the services needing attention regarding Scaling, Maturation and Hardening and recommending techniques for execution and working at the global level to help develop these recommendations. An example would be how current daily federation metadata operations are so human dependent and taking into account interfederation and more dynamic metadata, how such human dependencies might be eliminated.

Metrics Group

Metrics and linking FedOps metrics to Campus Metrics. The work would always have an eye towards operational needs as well as expressing metrics useful to demonstrate the value of all services. This would become an ongoing, standing work stream to define, interpret and report on Metrics for all services. The group would work with the Communications effort and the Service Development effort. It is suggested not to be a TAC activity but TAC members are likely to participate.

Expand Monitoring and Testing

Leverage, extend, and integrate work of Roland Hedberg, Leif Johansson, and Tom Scavo to

1. gather metrics
    1.1. deployed federating technologies
    1.2. deployed crypto-related algorithms
    1.3. compliance with standard protocols and profiles
2. identify potential issues
3. inform technical planning, both for InCommon operations and for participants

Campus IdP and SP Operators Group

Share tools and experiences, and develop requirements for federation software providers, addressing other operational concerns. This is suggested not to be a TAC activity but TAC members are likely to participate.

Managed Collaboration Service

Operate, contract, or coordinate the operation of a collaboration platform so that VOs and other collaborative activities have an alternative to doing so themselves.

- possible partners include HubZero, SURFconext, Globus Online, Perun (.cz), REMS (.fi)
- leverage COmanage, Grouper, and OpenConext development work

Provisioning Service

Provision accounts and groups to a growing set of SPs.

- offered as a service to campus IAM with a common API across supported SPs
    - could be the sole basis for InCommon membership, for some
- integrated with Managed IdP Service
- integrated with Managed Collaboration Service

3) Interfederation

o International
o Regional (see Point #6 below)
o Cross-sector
o Federal government

Implement the Interfederation TAC Subgroup Recommendations

1. Operationalize participation in eduGAIN and publicize the value
2. Operationalize bilateral interfederation agreements as identified by the subgroup
3. Fully participate in REFEDS. In particular, InCommon should always send representation to each REFEDS meeting
4. Review the Draft Code of Conduct for attribute release out of EU/EEA, and, if needed and possible, negotiate acceptable language changes.

Subfederation Model

- Establish at least one model for supporting or enabling R and/or E federations within the US to interoperate, so that an IdP user in any one can transact with an SP reachable by any other, access policy permitting.

US Federal SPs

- Develop an updated strategy for enabling InCommon participant access to identified US Federal SPs of interest to the Community.
    - May, but not necessarily, include FICAM or FCCX involvement
    - Will need to reconnect with agencies of interest: NSF, NIH, DoE, DoEd, NASA, DoD
    - Should be driven by specific use cases and access to services
- Align with R&E Assurance Needs Assessment item below.

4) Innovation, Influence and Leadership Where It Matters

o For example: REFEDS, NSTIC, IETF, OASIS, IIW, US Gov, TF-EMC2, FIDO, ISOC
o Middleware Software Development & Coordination

Take a Path-defining Role Regarding the Future of IAM for HE and Research

Campus CIO'sand VO leads regularly ask InCommon for information, guidance, and help in addressing their local on-campus IAM issues. They are usually seeking documentation, case studies, templates, and other tools to help them create a local roadmap for identity and access management. Ten years ago InCommon, via the NMI-EDIT grant, worked with a set of pilot schools to develop a similar package of information (The Enterprise Directory Implementation Roadmap). Since then, the problem has continued to evolve (eg handling new communities -- applicants, alumns, parents, online CE students, etc; dealing with mobile devices). CIOs seem to be asking for an updated and broadened version of that package.

In addition, many campuses find they are running locally developed IAM software that is 10-20 years old and which stopped meeting their evolving needs several years ago. However, they are not finding software in the marketplace that meets their IAM requirements. The CIFER project has started down the road to provide a suite of open source IAM software.

Because of these issues, this document recognizes two key overarching meta strategies.

1. Foster the creation of resources to assist campuses in the planning, deployment, and operation of their IAM systems. Providers of these resources include the InCommon membership, InCommon staff and volunteers, and InCommon's commercial partners.
2. Structure InCommon services in recognition of the fact that different InCommon member institutions will be at different maturity levels, each progressing at different rates. For example:

Institutions just getting started may rely primarily on social gateways to provide their community members with access to federated services that do not require any explicit sponsorship by the institution. Institutions at a somewhat higher maturity level will implement local Identity Providers (IdPs) that are capable of asserting institutional information about their community members, such as affiliation (student, faculty, staff, etc.) or entitlements for commercially-licensed services. Institutions at even higher maturity levels might implement multi-factor authentication or certify for federation-wide assurance profiles for access to higher-risk applications requiring high degrees of trust.

Assume an Active Role Supporting Local Campus IAM

Succeeding at Federation requires that a campus have an effective local IDM system. The two are strongly co-dependent. Many of the potential InCommon members will need to mature their existing IDM systems in order to obtain even basic value from Federation.

At the same time, many of InCommon's founding members are finding that their rapidly evolving IDM requirements are outstripping the functionality available in their 20-year old locally-developed proprietary IDM systems. These systems do not work well in a Federated world, where federated users need to be tracked and granted local permissions. Continuing Education and Certification programs are moving online, and creating significant new requirements in the IDM space.

Th CIFER effort is active in the space. But, there is a clear need to develop a clear message about CIFER. Is it a reference architecture that the community can use to influence the market? Or do we envision small, resource-strapped schools deploying an open source IDM solution? If not, then we need to work with commercial partners to ensure that their products work effectively in the Higher Education space. This is as much about leadership as technical strategy.

Charter a new InC Steering group, perhaps called "IAM Directions"

Mission/Goals/Deliverables of the proposed IAM Directions Group:

1. Identify gaps and emerging needs in IAM
    1.1. Develop a "Core IAM Capability and Function Model" to serve as a reference point for all group activities
    1.2. Document current IAM needs and requirements and approaches at a select handful of institutions ranging from small to large
2. Address those gaps and needs either directly or by coordination with other entities
    2.1. Track, advise pioneering IAM projects at collaboratively-minded institutions (e.g., CPR, OR)
    2.2. Draft project charters around specific sets of deliverables, document work plan and resource needs; forward to InC Steering for review/revision/approval
    2.3. Track approved and resourced IAM projects
3. Deliver solutions in the form of toolkits, recipes and case studies to the education and research community

3.1. Provide campus CIOs and VO leads with a roadmap showing federation and enterprise IAM strategic directions on a regular basis, including sequencing and a timeline. This roadmap should include the value for member institutions, as well as the expectations placed on those institutions.

3.2. Report to InC Steering periodically on "State of IAM"; keep the “IDM Landscape” document current and updated.

CIFER Work Teams have begun to address several of these items and have made significant progress in key areas. Cross-memberships and other forms of coordination with those teams might be the best path forward

Continue to Host Advance CAMP

- Re-establish a regular twice yearly IAM unconference with international and cross-sector participation.
- Internet2/InCommon event support plus sponsorship from other organizations.
- REFEDS and IETF adjacency for at least one annual ACAMP is important.

Foster Communication and Coordination with Other Groups in the IAM Space

For many years R. L. “Bob” Morgan served as Higher Education’s representative to the ever expanding set of groups operating in the IAM space. Some of these were neutral standards groups; others had a more clearly apparent proprietary interest. Bob travelled extensively, and participated in way too many conference calls. His knowledge, experience, and, most importantly, clear thinking and ability to see more of the future than others made him a welcome participant in many of these groups. Tragically, Bob died in July, 2012, leaving a big hole. There is no one who can step in and replace him in his many roles, and with his many connections.

That said, InCommon needs a strategy for raising its level of participation in many of those groups and arenas, and in ensuring that there is adequate internal communication and information flow about what is being discussed outside of InCommon.

- Example groups: REFEDS, NSTIC, IETF, OASIS, IIW, US Gov, TF-EMC2, FIDO, ISOC
- Start by defining, group by group, what kind of relationship would be of greatest mutual benefit
- Identify individuals in our community who can act as two-way liaisons with each targeted group
- Share information on key achievements and activities with our community as we learn of them

5) Putting Trust & Privacy into Identity

o Refining Assurance Program to meet our needs
o Multifactor Authentication (MFA)

o Building a privacy infrastructure (end entity categories, user consent tools)

The InCommon Community has worked with an array of US Federal Agencies over the last ten years to find a practical path that would allow campus community members to use Federation to access Agency services. There has been moderate success with low-risk services, but despite substantial effort to develop and deploy an Assurance Program, uptake has been extremely low due to the lack of Agency services requiring it.

Within InCommon Community, though, there is an increasing need to find a practical strategy for accessing higher risk services not offered by the US Government. It may be time for Higher Ed to develop its own Assurance Profiles, addressing the Community needs, rather than building on the US government requirements.

R&E Assurance Needs Assessment

Convene community group to identify valuable uses for trust & privacy related programs, documents, services, and products in the R&E sector

1. campuses: administration, system and data security
2. adjacent communities and organizations: K12, DoE, DoEd, NIH, NSF
3. scientific and scholarly cyberinfrastructure
4. virtual organizations and VO support organizations
5. partner with Center for Trustworthy Scientific Cyberinfrastructure

R&E Specific Assurance Profile

- Building upon (or in parallel with) the R&E Assurance Needs Assessment, define the first US R&E assurance profile responsive to R&E assurance needs.
- the assurance profile should not be constrained by US FICAM assurance and privacy program

Leverage Multi-Factor Cohortium

- assemble use cases, deployment experiences, technology options into an “MFA Roadmap” for campuses

Trust elevation for social credentials

- Track work going on in standards groups
- Track pilots exploring various mechanisms

Shibboleth Trust & Privacy Enhancements

- put user consent tool into Shibboleth development roadmap
- evolve Multi Context Broker specifications in response to field experiences
- documentation/video/training on using Shibboleth’s trust & privacy capabilities

Raise the Bar for Operating an Entity with InCommon

1. Raise the participation bar for operating an IdP within InCommon (e.g., info that each member must publish or provide), so that other members can more easily interoperate with them

2. Develop and provide best practice information for managing identities and Assurance for both non-credit and credit online courses
3. Develop some recommended practices related to trust elevation (particularly with respect to social accounts)
4. Review the process of becoming a Sponsored Partner with an eye towards increasing the value of vendor services
5. Implement a tagging system or certification program that identifies Sponsored Partners that meet certain requirements and/or recommended practices

Make (Some Level of) Privacy Possible

1. Work with campuses to develop a new consensus around the meaning and practice of privacy
2. Deploy a Federation-based infrastructure supporting privacy (end entity categories, RequestedAttribute elements, user consent tools, approach for attribute aggregation (eg NAME))
3. Integrate user consent tool into Managed IdP Service (note that this will likely require significant evolution of the deployed infrastructure).
4. Provide a downloadable IdP install package that includes the tools for managing personal privacy

Leverage Certificate Service

1. Finish development/deployment of InCommon IGTF Server CA serving cyberinfrastructure providers' need for IGTF compliant certificates (requested by XSEDE).
2. Encourage and support use of InCommon client certificates for user authentication to campus IdPs (with InCert easing client certificate deployment) for phishing protection and 2FA.
3. Encourage and support use of InCommon EV certs on IdP login pages for higher assurance.
4. Work with the vendor to deploy Federated access to the Certificate Manager service.
5. With the renewal of the certificate services contract looming, work through an RFP process to identify potential opportunities for new technology and/or improved pricing or services.

6) Teaching and Learning Support

o K12 synergies
o High value services: LMS system integration

K12 synergies

Partner with Network Regionals and the Quilt to Conduct Pilots to Bring Federation to K12

1. 8 State-based Pilots underway
    1.1. Identify Federation requirements and develop most common use cases including delegated business and technology roles in addition to classic interfederation.

1.1.1. Leverage existing relationships, business processes, and technology infrastructure to develop business models that address the use cases while reducing the cost to join and operate in InCommon for k12.
1.1.2. Address the classic interfederation use cases using the TAC subcommittee for those states that will be running their own separate federation.
1.1.3. Pilot one business model with a Regional Network
1.2. Summarize lessons learned
2. Conduct Second round of pilots in 2014
2.1. Use lessons learned to jumpstart next round
2.2. If successful, develop piloted business model into Regional Partnership offering.

High value services: LMS system integration

- Align SAML and IMS LTI on handoff from LMS (as LTI Tool Consumer) to an LTI Tool Provider
    - Goal: Promote changes to IMS LTI specification to leverage SAML Request Initiation Protocol
    - Tactic: Get an LTI Tool provider and an LMS to implement the modified approach, work through LTI sponsors to get changes into the spec

K12 Access to Campus-based Services (application and transfer processes)

- InCommon should continue participating on the CommIT project to develop the business, policy, and technical models for an IdP serving members of the K12 community accessing Higher Ed SPs. A primary outcome includes a K12 facing IdP that students can use to apply to HE institutions.

7) Research Support

o Outreach
o Collaboration Services
o Two more major research projects using COmanage(?)

Research Support Group

Goals:
1. Provide visible, first class support for research applications in InCommon.
2. Bring research communities together to achieve critical mass to identify common needs and effectively engage with hundreds of InCommon IdPs and international federations.
3. Actively promote InCommon to research communities, bring research communities into InCommon, and help them quickly gain value from InCommon.
4. Enable research communities to leverage InCommon for interoperable identity management rather than rolling their own.

Target Metrics:
1. % of US HE InCommon IdPs that support R&S. 2014 target: 90% (currently 19%)
2. # of InCommon R&S SPs. 2014 target: 30 (currently 15)

3. # of documented research support success stories. 2014 target: 4
4. # of unique users accessing research applications via InCommon. 2014 target: 100,000

Strategies/Tactics:

1. Significant allocation of staff to research application support is critical to demonstrate real commitment by InCommon to meeting the needs of the research community. Anything less than 1.0 FTE dedicated to research application/community outreach/support would be taken as a sign by the research community that research applications continue to be a low priority for InCommon.
2. Provide a forum for research-focused IdPs and SPs to share challenges and successes with each other and with InCommon staff who have time allocated to assist with solving challenges, spreading the word about successes, and otherwise supporting/encouraging/promoting research applications in InCommon.
    2.1. Publicly archived email list -- a visible sign to research groups considering InCommon that there is an active community around research applications in InCommon
    2.2. Regularly scheduled telecons
    2.3. Webinars, workshops, tutorials
    2.4. Wiki space: how-to docs, success stories
3. Increase the visibility of research applications in InCommon. Help InCommon IdPs see the value in supporting research applications.
4. Present and advertise at research conferences: Supercomputing, OSG AHM, XSEDE, AGU FM, etc.
5. Provide federation services targeted to research apps: R&S, Google Gateway, IdP of Last Resort, collaboration and provisioning services, multifactor services, etc. See below for specific suggestions targeted at R&S services.
6. InCommon staff actively soliciting research community participation in InCommon
    6.1. Identifying funded research projects
    6.2. Identifying research communities on InCommon-member campuses
7. InCommon staff actively promoting support for researcher needs by InCommon IdPs
8. Initial target research communities: LIGO, GENI, HubZero, XSEDE (campus champions), OSG (CIC), iPlant, DataONE, Science DMZ, Open Science Data Cloud, I2 HENP SIG, …
9. Potential partners: Globus, XSEDE, CILogon, CTSC, …
10. Engage NSF/NIH regarding newly funded projects and endorsement of an identity-enabled collaboration platform
11. A Federation-based service that a research project could contact; the project would pass along the names of member campuses, and the service would contact non-IC members and encourage and support them to operate an IdP

ECP Support for R&S

Deploy a Research Community IdP (an IdP of Last Resort) with ECP capability for R&S SPs.

Google Gateway Support for R&S

Expand the Internet2 Google Gateway service to include R&S SPs.

Multifactor Support for R&S

Provide a multifactor authentication service targeted at R&S SPs.