Response to the Department of Commerce Notice of Inquiry
for
**Models for a Governance Structure for
the National Strategy for Trusted Identities in Cyberspace**

EDUCAUSE, Internet2 and InCommon
July 22, 2011

EDUCAUSE, Internet2 and InCommon are pleased to provide responses to the questions raised in the Department of Commerce Notice of Inquiry (NOI). Our organizations represent a significant portion of the academic and research communities in the United States. Our membership has considerable experience with information technology governance, policy, privacy, and identity management issues.

The research and education community is comprises of over 4,000 not-for-profit colleges and universities, over 2,000 for-profit institutions, and a variety of government-funded and privately supported or operated research entities. Collectively, the postsecondary educational community educates the workforce, facilitates research and discovery, and operates some of the most powerful and sophisticated computer networks in the world. Consequently, there is a vast amount of experience and expertise in academia, ranging from faculty who research and write on subject matters such as computer science, cybersecurity, identity management, and privacy to the professional IT staff who operate campus core technologies including the identity and access management infrastructure. EDUCAUSE, Internet2, and InCommon represent that practitioner community within higher education who must be recognized as critical partners in the successful realization of the vision and goals of the National Strategy for Trusted Identities in Cyberspace (NSTIC).

Our organizations have discussed the questions raised by the NOI and have participated in several meetings and workshops sponsored by the NSTIC Program Office (NPO). We offer herein our considered responses to the important questions raised by the NPO NOI and look forward to contributing to the next steps in this important work.

We applaud the vision and foresight of the leadership of the NSTIC initiative for articulating the four guiding principles that will guide development of the long-term strategy and deployment. That vision requires that identity solutions must be:

- privacy-enhancing and voluntary,
- secure and resilient,

- interoperable, and
- cost-effective and easy to use.

In addition to our specific responses below, we would like to offer some higher-level observations that we hope may be instructive and constructive. These are informed by our organizations' long experience with information technologies, understanding of our diverse communities, and our support for an identity federation that is a prototype of the sort of identity ecosystem envisioned by the NSTIC.

We are concerned that the NSTIC vision may be overly ambitious in scope and scale and the resulting complexity could mean that it will take many years to come to fruition. The desired inclusiveness brings with it potential for a no-win situation. Trying to reconcile differences among a variety of stakeholders is a major undertaking: some may not want the NSTIC to succeed; others may have widely differing goals. The lack of a legal framework for managing trust in cyberspace could make finding common ground extremely difficult. Perhaps an incremental approach that addresses a significant but more narrowly scoped set of current problems could both demonstrate the usefulness of the identity ecosystem and provide opportunity to learn more about some of the obstacles that confront us, test new solutions, and refine the rules to meet new challenges..

Another concern is the enforceability of NSTIC decisions. As a private sector organization, the governance body will have to rely on contract law to hold implementers accountable; the result could lead to a voluntary system where implementers would be free to implement NSTIC recommendations as written, or not. Therefore, we believe the Federal government must have some limited and clear role beyond participating as one of the equal stakeholders. Sponsoring and shepherding adoption of NSTIC decisions through the democratic political processes (i.e., legislation, regulation, standards, guidance, etc.) rather than by means of bureaucratic structures, would be a far more generally acceptable way to resolve fundamental issues of public policy such as privacy, security, and accountability.

In consideration of the above, we believe it would be wise for the steering group to focus initially on principles subordinate to or in addition to the four guiding principles already stated in NSTIC and rules that embody those principles. For example, the European Union (EU) Article 29 Data Protection Working Party[1] rules have articulated important principles governing the management and handling of personally identifying information instead of prescribed procedures or implementations. While some of these rules have proven cumbersome or ambiguous in practice, the model of rules versus prescriptions encourages innovation and allows for new solutions as technology and use cases evolve.

Another important principle is that all technology or standards developed under the NSTIC effort must be "open source" and freely available to all, particularly those relevant to cryptography intended to ensure security of sensitive information. This would promote both competitive implementation and consumer trust in the evolving ecosystem.

In our responses below, we have tried to balance the various, and sometimes competing, priorities of the various stakeholders. We bring to this NOI both our years of experience building and operating online identity services from within and on behalf of the academic and research community.

---

[1] See http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

Responses to the Notice of Inquiry questions

---

1. Structure of the Steering Group

There are many models of governance that perform some of the wide range of functions needed to formulate and administer the Identity Ecosystem Framework. While not all of these functions are unique to the steering group, few examples of governance cover the same breadth of the technical and economic landscape as the Identity Ecosystem Framework. The steering group, therefore, has a greater risk of either being too small to serve its purpose, or too large to govern effectively. There is a full spectrum of affected economic sectors, some of which are highly-regulated and some of which are unregulated. The steering group will need to simultaneously integrate the Identity Ecosystem Framework with regulatory requirements faced by firms in a variety of industry sectors. At the same time, the steering group needs to consider and represent the interest of the broader public in security and privacy. It is imperative to find a working structure that accomplishes all these needs.

Questions:

> 1.1. Given the Guiding Principles outlined in the Strategy, what should be the structure of the steering group? What structures can support the technical, policy, legal, and operational aspects of the Identity Ecosystem without stifling innovation?

The term "governance" may too strongly state what is needed for the NSTIC effort to succeed. Rather, a "steering group," "coordinating body," or "working group" that can facilitate communication, planning, and action among and between existing or new organizations may be a more appropriate model to pursue. What is needed is an effective public-private partnership between government (federal, state, and local) and private sector organizations (to include both for-profit and not-for-profit entities). Leadership from the private sector is an essential precondition for the success of NSTIC.

Another consideration for the steering group is the type of expertise that will be necessary for effective implementation of NSTIC. The InCommon Federation provides an example of how that might be accomplished. The InCommon Steering Committee is concerned with the governance, policy, and business operations of the organization. The Steering Committee is comprised of college, university and research agency chief information officers and sponsored partner representatives. A Technical Advisory Committee consisting of college and university IT architects and identity management specialists is concerned with technology, operational practices, and standards for federated identity management. Specialized *ad hoc* working groups are sometimes established for accomplishing specific goals and producing concrete outcomes. While the two groups (steering and technical) have served InCommon well, there is also a recognition that other viewpoints are necessary including legal expertise, policy experience, privacy advocacy, representation of small and large institutions, and so forth. To the extent possible, care is taken to represent diverse experiences and institutional types on the steering and other committees.

It is clear that the Steering Group (SG) must be both agile and broadly informed. The decision-making body of the SG should consist of highly knowledgeable and experienced individuals representing major stakeholder communities, including consumers, business, public policy, government, and academia and research. All members should have, in

addition to his or her own field or specialty, cross-cutting knowledge in other aspects of the identity ecosystem.

To remain modest in size and also effective, the SG will need to receive a great deal of advice from highly active subordinate working groups (WGs) that can make specific recommendations in areas such as technology, legal, legislative and regulatory matters, and public policy including privacy and personal choice issues.

To avoid stifling innovation, the work of the SG should focus on policy, principles, new standards where needed, and guidelines. The range of use cases and contexts in which online identity is or will become important is a very wide. Prescriptive solutions are unlikely to be effective across this entire spectrum.

> 1.2. Are there broad, multi-sector examples of governance structures that match the scale of the steering group? If so, what makes them successful or unsuccessful? What challenges do they face?

One existing model is the Partnership for Critical Infrastructure Security (PCIS), which was created by Homeland Security Presidential Decision Directive 7 in 2005. Although the stakeholders that are part of the PCIS (i.e., those designated as "critical infrastructures") may be too limiting for NSTIC, the model does bring together various sectors of the economy for a common purpose, despite the diversity among the sectors (including the varied nature of regulation by sector). Additionally, the PCIS has established a Cross-Sector Cyber Security Working Group (CSCSWG), which is representative of the stakeholders (even broader than "critical infrastructures"). The CSCSWG establishes project teams as needed to pursue new initiatives, holds monthly meetings for organizational updates and project status reports, and seeks to promote cooperation and collaboration among and between both the public and private sector stakeholders. The CSCSWG is co-chaired by private sector representatives; meetings are coordinated and hosted by the U.S. Department of Homeland Security. While it is not a perfect model for NSTIC, it produces the kind of communication and voluntary participation that would be useful in advancing NSTIC.

The Auditing Standards Board is another such organization. It is a private sector group that is effective, in part, because adherence to its recommendations is required by the SEC.

Another example is the U.S. health care system. This public-private partnership sets requirements for licensing of practitioners and facilities and is supported by innovative, market-driven funding.

The Smart Grid Interoperability Panel (SGIP) has been mentioned in discussions as a possible model for the NSTIC SG and is worth studying. Our concern with that suggestion is that the SGIP is focused on a more narrow engineering problem with little need for participation by citizens or even other sectors. These concerns may require significant adaptation to make the SGIP model effective.

> 1.3. Are there functions of the steering group listed in this Notice that should not be part of the steering group's activities? Please explain why they are not essential components of Identity Ecosystem Governance.

We see nothing inappropriate in the activities listed.

> 1.4. Are there functions that the steering group must have that are not listed in this notice? How do your suggested governance structures allow for inclusion of these additional

functions?

As mentioned above, one strong concern is the enforceability of SG decisions, standards, policy, and the like. What mechanism or authority will the SG have to obtain government support for its actions?

Undoubtedly, the charter of the SG will need to evolve with experience and may need to add functions as such needs arise. Perhaps this should be a bi-annual function required of the SG. Therefore, thought must be given initially to how such authority and responsibility can be changed appropriately in the future.

> 1.5. To what extent does the steering group need to support different sectors differently?

The SG must have a stable funding source both to support its basic operations and to provide need-based subsidies to stakeholder representatives who would otherwise be unable to participate. Some SG or WG members may need to travel to international conferences or work groups (per section 4 below). Flexibility is essential to ensure that certain stakeholder groups are not disenfranchised.

> 1.6. How can the steering group effectively set its own policies for all Identity Ecosystem participants without risking conflict with rules set in regulated industries? To what extent can the government mitigate risks associated with this complexity?

The SG must accommodate the rules within regulated industries if it is to succeed. For example, the Accounting Standards Board (ASB) has developed different—but related—accounting standards for different sectors. The SG must have access to regulatory experts for advice and may need to suggest changes to some regulations if there is a strong, broadly supported case to do so.

> 1.7. To what extent can each of the Guiding Principles of the Strategy–interoperability, security, privacy and ease of use—be supported without risking "pull through" regulation from regulated participants in the Identity Ecosystem?

As mentioned above, the ASB has demonstrated that this can be accommodated. Clearly the SG would have an interest in reviewing any such regulations that might impede adherence to the fundamental guiding principles. Multi-sector representation on the SG or on the WGs is critical to ensuring that the needs of the different sectors are considered.

> 1.8. What are the most important characteristics (e.g., standards and technical capabilities, rulemaking authority, representational structure, etc.) of the steering group?

The SG must establish a system that is trusted by all parties, especially by the general public. Therefore, the most important characteristic is a willingness to pursue the "greater good" rather than narrow interests of a few stakeholders. To be successful, the SG must work to understand the interaction between policy and technology and the longer-term consequences for all players in the ecosystem.

The process and rules governing decision-making is a critical decision. No one stakeholder community should be able to either veto or hold sway over others. Representation must be as equal as feasible and significant decisions should require a supermajority (e.g., 75% affirmative).

The breadth of knowledge and experience of SG members is also critical. If the initial SG membership is to be appointed by the NPO, the NPO should create a set of generic

guidelines regarding qualifications to avoid any appearance of bias as well as to ensure highly capable and effective membership.

Rulemaking authority is the primary reason that groups would ultimately participate in and support the work of the SG.

> 1.9. How should the government be involved in the steering group at steady state? What are the advantages and disadvantages of different levels of government involvement?

Government at both the state and federal level must be represented on the SG as a stakeholder community. Federal and state agencies offer online services that could be highly sensitive to identity fraud. In addition, law enforcement and emergency responders need to rely on strong identity both online and off-line. Government representation should be no more or less powerful than that for any other stakeholder community.

Federal NPO-managed funding should be made available for the initial SG and should continue until or unless a long-term, stable, non-Federal source is established. It is critical that funding for this activity be sufficient yet not influence the membership or decisions of the SG.

---

2. Steering Group Initiation

In its role of supporting the private sector's leadership of the Identity Ecosystem, the government's aim is to accelerate establishment of a steering group that will uphold the Guiding Principles of the Strategy. The government thus seeks comment on the ways in which it can be a catalyst to the establishment of the steering group.

There are many means by which the steering group could be formed, and such structures generally fall into three broad categories:

> a) A new organization, organically formed by interested stakeholders.

> b) An existing stakeholder organization that establishes the steering group as part of its activities.

> c) Use of government authorities, such as the Federal Advisory Committee Act (FACA), to charge a new or existing advisory panel with formulating recommendations for the initial policy and technical framework for the Identity Ecosystem, allowing for a transition to a private sector body after establishing a sustainable Identity Ecosystem, or through the legislative process.

Questions:

> 2.1. How does the functioning of the steering group relate to the method by which it was initiated? Does the scope of authority depend on the method? What examples are there from each of the broad categories above or from other methods? What are the advantages or disadvantages of different methods?

The NSTIC is not primarily a market-based problem; it is a public policy problem. If adherence to the four guiding principles is to be ensured, the NPO must be the initiator of the SG. Any existing "stakeholder" will be seen as biased and a "new, organically formed" organization is unlikely to be adequately broad-based, balanced, and committed to the strategic guiding principles. Therefore, some form of option c) above seems most

promising. However, the initial SG instantiation must be an open and transparent process with attention paid to concerns raised by any stakeholder community.

One approach is to have the government initiate the NSTIC SG but in the charge to the initial SG that defines their activities to set a definitive date in the future for transitioning this to a nongovernmental organization. The charter would provide the government initial authority to set the ground rules but force it to stand up a new structure in a timely manner, for example, by December 31, 2014.

> 2.2. While the steering group will ultimately be private sector-led regardless of how it is established, to what extent does government leadership of the group's initial phase increase or decrease the likelihood of the Strategy's success?

Leadership in terms of operational and infrastructure support is essential; leadership in terms of decision-making must be limited to ensuring adherence to the four strategic principles. The government must not be seen as imposing a particular outcome on the SG.

We would point to the birth and evolution of the Internet as an extremely successful example of an "ecosystem" that was developed with initial Federal funding in the late 1960s and became fully self-supporting in the private sector by the mid-1990s. The Federal government's leadership in the initial-phase was essential and also light-handed. The public-private partnership has worked extremely well.

> 2.3. How can the government be most effective in accelerating the development and ultimate success of the Identity Ecosystem?

The government must focus on bringing together the divergent parties and establishing the frameworks and boundaries for addressing essential privacy and security concerns. Without setting an achievable scope and clear ground rules, development of the identity ecosystem could be prolonged or fail altogether.

In our experience, organizations that depend on volunteers for significant work products are very slow to produce results. We believe that funding full- or part-time positions to support the work of the SG and/or WGs would significantly enhance the development and ultimate success of the identity ecosystem.

> 2.4. Do certain methods of establishing the steering group create greater risks to the Guiding Principles? What measures can best mitigate those risks? What role can the government play to help to ensure the Guiding Principles are upheld?

As suggested above, the one role unique to the government (NPO) in the SG should be to ensure adherence to the guiding principles. This might best be accomplished through a veto power that should be used judiciously and only when all attempts at consensus or compromise have been exhausted.

It is worth mentioning the significant and powerful tension between protecting personal privacy and the desires of the marketplace to monetize personal identity. Therefore, the market alone is unlikely to force commercial entities to adhere to the guiding principles. Allowing the SG to become dominated by commercial interests would create an untenable environment. There may be a need for some limited form of government regulation over critical aspects of the ecosystem, legal recourse for people who have been injured, and substantial penalties for parties that abuse the rules.

2.5. What types of arrangements would allow for both an initial government role and, if initially led by the government, a transition to private sector leadership in the steering group? If possible, please give examples of such arrangements and their positive and negative attributes.

As suggested above, initial funding for operation of the SG and, as needed, its membership could be conditional on the SG actively developing an independent, long-term stable funding source. Leadership of the SG activity need not be a role for the NPO if a strong membership and decision-making structure is created before initiation of the SG.

We again point to the Internet as a highly successful example of a government initiative that was transitioned to the private sector. In the early phases of the Internet, development was an open-process guided by "peer reviewed standards and working code." Standards that showed sufficient merit succeeded. That precedent still prevails in the continuing evolution of the Internet.

---

3. Representation of Stakeholders in the Steering Group

Representation of all stakeholders is a difficult but essential task when stakeholders are as numerous and diverse as those in the Identity Ecosystem. The breadth of stakeholder representation and the voice they have in policy formulation must be fair and transparent. The steering group must be accountable to all participants in the Identity Ecosystem, including individuals. An essential task for the steering group will be to provide organizations or individuals who may not be direct participants in the Identity Ecosystem, such as privacy and civil liberties advocacy groups, with a meaningful way to have an impact on policy formulation.

Given the diverse, multi-sector set of stakeholders in the Identity Ecosystem, representation in the steering group must be carefully balanced. Should the influence skew in any direction, stakeholders may quickly lose confidence in the ability of the steering group to fairly formulate solutions to the variety of issues that surround the creation and governance of the Identity Ecosystem.

Questions:

3.1. What should the make-up of the steering group look like? What is the best way to engage organizations playing each role in the Identity Ecosystem, including individuals?

The role of the SG is to ensure adherence to the four guiding principles in adoption of all standards, solutions, and processes that form the identity ecosystem. Potential issues do not revolve primarily around how to accomplish a goal but instead around what parties accept the risks involved.

Three primary stakeholder categories will be affected: individuals whose privacy and property may be put at risk; suppliers and consumers of goods and services whose income or resources may be put at risk; and identity providers who may be liable for losses incurred by other parties if the identity ecosystem fails to function properly.

Each of these stakeholder categories is represented by numerous existing advocacy groups and these should be strongly represented in the SG. It is unclear whether or how "individuals" *per se* can be represented except perhaps on some of the subordinate WGs where their expertise may be valuable. Instead, advocacy groups such as the American

Association of Retired People (AARP), and the Consumers Union could be enrolled to represent the concerns and needs of individuals.

In addition, the SG should include or have strong WGs to represent the legal, audit, and assessor communities. Understanding how SG-established rules can be woven into existing legal structures and precedents is essential to success. Understanding how auditors and assessors can reliably certify identity providers and relying parties is critical to establishing broad trust in the ecosystem.

The SG, of course, is composed of individuals whose expertise can contribute to the best outcomes but who also represent the needs and concerns of stakeholders. Organizations that wish to contribute to the development of the identity ecosystem should be required to make a strong case for their involvement and also nominate individuals whose particular expertise and experience are of demonstrable value to the overall work of the SG.

With respect to academia, bear in mind that while faculty and researchers may be disciplinary experts, they may not have practical experience with identity management systems or have served in a role as owner or operator of them, in contrast to the members of EDUCAUSE, Internet2, and InCommon. Therefore, we must ensure that the role of "academia" for the purposes of NSTIC includes the professional IT staff of colleges and universities.

> 3.2. How should interested entities that do not directly participate in the Identity Ecosystem receive representation in the steering group?

Entities that have relevant expertise should be encouraged to participate in one or more WGs instead of the SG itself.

> 3.3. What does balanced representation mean and how can it be achieved? What steps can be taken guard against disproportionate influence over policy formulation?

In our view, "balanced" will be determined by what is being weighed. It might mean that no one constituency or stakeholder group has greater representation than others but that concept is ill-defined as well. Instead, we believe the SG should have strong representation from each significant stakeholder group and from infrastructure and service providers that have demonstrated experience in defining, developing, and supporting various aspects of the current identity ecosystem. Disproportionate influence can be mitigated by requiring supermajority affirmative voting, e.g., 75%, on all major decisions.

Representation should include at least the following general groups:

- Representatives of particularly risk sensitive sectors, e.g., the financial industry broadly (banking, investment, credit and mortgage, etc.); the healthcare providers and supporting entities (hospitals, pharmacy, medical drug & research), etc.;

- Business-to-business advocates and developers;

- Business-to-consumer advocates and developers;

- Identity credentialing and attribute service providers, e.g., InCommon, Google, PayPal, etc.;

- Consumer privacy and legal rights organizations, e.g., Consumers Union, ACLU, etc.;

- State and Federal government (representing concerns of law enforcement, national

security, electronic voting, etc.);

- Information technologists and IT providers to bridge the gap between theory and practice.

In addition, standards bodies such as the American National Standards Association (ANSI), legal bodies such as the American Bar Association (ABA), and audit and certification bodies such as ISACA[2] should be advisory to the SG.

3.4. Should there be a fee for representatives in the steering group? Are there appropriate tiered systems for fees that will prevent "pricing out" organizations, including individuals?

Fees, tiered or not, would represent a barrier for some stakeholder groups. Initial funding for this work should come from the NPO until a long-term, stable funding model can be created. In particular, "ability to pay" must not be a factor in determining the composition of the SG.

3.5. Other than fees, are there other means to maintain a governance body in the long term? If possible, please give examples of existing structures and their positive and negative attributes.

An independent fund manager might be created to accept NPO appropriations and tax-deductible donations from any legitimate source. The SG would not be given any information that could identify specific donors or sources.

Another possible model might be fees charge to the regulated entities, in a way similar to how the SEC is funded.

3.6. Should all members have the same voting rights on all issues, or should voting rights be adjusted to favor those most impacted by a decision?

Voting influence should be equal for all members but decisions with significant impact must be made by a supermajority (e.g., 75%, affirmative vote). Any significant decision may have positive or negative impact on certain stakeholders. That concern should not override the goal of making the best possible decision on every issue before the SG.

3.7. How can appropriately broad representation within the steering group be ensured? To what extent and in what ways must the Federal government, as well as State, local, tribal, territorial, and foreign governments be involved at the outset?

Broad representation would be achieved by obtaining representation from all the stakeholder groups identified in response to question 3.3 above. In addition, other stakeholder groups may submit a case to the NPO for their inclusion. Governmental entities should participate from the outset, as they represent a critical stakeholder group.

Rather than too narrow representation, the risk might be too diffuse representation. Members of the SG must be consensus builders, not intransigent position holders. We encourage the NPO to develop generic guidelines for participants and participation in the SG.

---

[2] See http://www.isaca.org/

Questions:

4.1. How should the structure of the steering group address international perspectives, standards, policies, best practices, etc?

Each WG under the SG should be responsible for coordinating its work with any relevant international body. Many U.S. entities already participate in the International Telecommunication Union Technical Standardization Sector (ITU-T), the International Organization for Standardization (ISO) and other such activities. Participants would inform WGs of relevant activities. Each WG should include at least one member of the SG to bring garnered perspective to the SG most effectively.

4.2. How should the steering group coordinate with other international entities (e.g., standards and policy development organizations, trade organizations, foreign governments)?

In addition to what we have suggested above, members of the SG may wish to meet with leadership of such international bodies to clarify goals and issues as needs arise.

4.3. On what international entities should the steering group focus its attention and activities?

One clear example is the EU Article 29 Data Protection Working Party, as mentioned above. Another example is the working group of Research and Education Federations (REFEDS) which represents "the requirements of research and education in the ever-growing space of access and identity management, working with and influencing the direction of organisations such as Kantara, OIX and Identity Commons on behalf of our [European] participants."[3]

4.4. How should the steering group maximize the Identity Ecosystem's interoperability internationally?

The SG also must recognize international and cultural differences in what "identity" means, how it is established or verified, and what norms or regulations govern its management and use. Notions or provenance and authority must be understood and equivalencies defined for international use.

---

[3] See http://refeds.org/

Diplomacy, consultation, collaboration, and compromise will be needed. The United States must not be seen as a heavy-handed player intent on forcing a solution upon the rest of the world.

> 4.5. What is the Federal government's role in promoting international cooperation within the Identity Ecosystem?

If an identity ecosystem is to be truly international, then the United Nations should create an organizational component to oversee issues that arise. As NSTIC evolves, it may become necessary to establish international agreements or treaties for certain high level-activities that can be addressed only by the Federal government.

Summary

There are examples today of standards and technology that are already working or that could evolve into significant parts of the envisioned identity ecosystem. We believe it is important that the experience gained from these existing efforts be incorporated into the work of the NSTIC SG.

A well supported NPO that can establish a stable, broadly representative SG with active, expert WGs as advisory to it will have the best chance of success in this complex and difficult initiative.

Signatories

The signatories to this submittal represent long standing, major organizations with a great deal of experience in digital identity management and a strong interest in the intent and success of the NSTIC vision. Our organizations represent 25+ million individuals in 4,000+ academic and research institutions.

Gregory Jackson	H. David Lambert	John J. Suess
Vice President	President and CEO	Steering Committee Chair
EDUCAUSE	Internet2	InCommon

About EDUCAUSE

EDUCAUSE is a nonprofit association and the foremost community of IT leaders and professionals committed to advancing higher education. EDUCAUSE programs and services are focused on analysis, advocacy, community building, professional development, and knowledge creation because IT plays a transformative role in higher education. EDUCAUSE supports those who lead, manage, and use information technology through a comprehensive range of resources and activities. For more information, see www.educause.edu.

About Internet2

Internet2 is an advanced networking consortium led by the research and education community. An exceptional partnership spanning U.S. and international institutions that are leaders in the worlds of research, academia, industry and government, Internet2 is developing breakthrough cyberinfrastructure technologies that support the most exacting applications of today—and spark the most essential innovations of tomorrow. Led by its members and focused on their current and future networking needs since 1996, Internet2 blends its human, IP, and optical networks to develop and deploy revolutionary Internet technologies. Activating the same partnerships that produced today's Internet, the Internet2 community is forging the Internet of the future. For more information, see http://www.internet2.edu.

About InCommon

InCommon, operated by Internet2, offers a common framework of trust services to its members—institutions of higher education, federal agencies, and research organizations—as well as their corporate partners. InCommon operates the InCommon Federation, the U.S. identity management federation for research and education, and the InCommon Certificate Service. For more information, see http://www.incommon.org/