INTERNET2

INCOMMON OPERATIONS REVIEW FINDINGS AND RECOMMENDATIONS

Report prepared 2015.09.24 by Nicholas Roy, Director of Technology and Strategy, InCommon
With input and assistance from: Ann West, Steve Zoppi, Paul Caskey, Mike LaHaye, Tom Scavo, John Krienke, Angi Sizemore, IJ Kim, Jeff Hagley, Ryan Nobrega, Ryan Martin

TABLE OF CONTENTS

BACKGROUND

At the request of the Associate Vice Presidents for Trust and Identity (Ann West) and Services Integration and Architecture (Steve Zoppi), and with the support of the Senior Vice President for NET+ Services (Shelton Waggener), the Director of Technology and Strategy for InCommon (Nick Roy) was assigned to develop a framework for the operational review of InCommon services (the InCommon Federation and Certificate Service), and to conduct an operational review to determine any service delivery gaps which could prevent continued, scalable, supportable and manageable growth of existing InCommon services; the development of new services; and the long-term support of mission-critical identity infrastructure for the US and international Research and Education sector, which InCommon now provides. This report serves as the primary deliverable from that review process, and is intended as a tool for decision-making with regard to the findings contained therein.

EXECUTIVE SUMMARY

InCommon has grown over its approximately 10 year history from a semi-experimental best-effort “identity club” - as originally envisioned by the Middleware Architecture Committee for Education (MACE), into a suite of mission-critical Trust and Identity services offered to the US and international Research and Education sector, and an interconnected peer among similar such service offerings globally. It has succeeded beyond the greatest hopes of its pioneering architects and first participants, growing from the Federation service and a limited set of R1 institutional founders, to a diversity of services with a majority membership of smaller institutions with a different set of needs and requirements. Many of today's InCommon Participants are not members of Internet2. The Federation and Certificate Services have become critical infrastructure for the participants who in turn deploy high value institutional and cross-organization services which depend on these InCommon services.

In the context of this growth and evolution in service offerings, and with many new service offerings with different service support and technical requirements, it will be necessary to appropriately resource and manage InCommon to meet the needs of the next decade and beyond.

InCommon currently operates as a set of service offerings which are managed by a small staff using processes, technologies, and support models that are straining under the weight of today’s increasing demands. The current support model cannot hope to sustainably support future needs, and indeed shows signs of risk of failure to deliver on current expectations.

For these reasons, this report recommends a holistic approach to service management based on a relatively lightweight service delivery framework; analysis of staffing roles and levels and some new and modified roles and responsibilities with InCommon and Internet2; the addition of and development of rigor around use of appropriate service management tools, technologies and processes; and the possible need to differently source technical operations to meet existing and emerging needs. Detail on the specific recommendations is contained in the section “Desired State, Gaps and Remedies,” below.

METHODOLOGY

The Microsoft Operations Framework (MOF) v4 was selected as a relatively lightweight and non-prescriptive operations, service delivery and planning framework to use as a basis for an assessment tool and review process. This framework is successfully used by many large IT organizations for IT service planning, governance, delivery, operation and assessment.

Because InCommon services were not designed using a service framework, components of a typical service design and delivery cycle (in the MOF, “Plan,” “Deliver,” and “Operate” phases) have not been in place. For this reason, it was necessary to design a custom version of an “Operational Health Management Review.” This review is typically very limited in scope, focuses only on the day-to-day operations of a single service offering, and may focus only on identified aspects of review for the service delivery of this single service offering.

The need for this initial operations review of InCommon was much broader in scope, and required up-front input from members of technical, security, service management and service operations staff in order to collect documentation, document known gaps, highlight and provide overviews of existing processes, and review the compiled documentation ahead of an in-person two-day meeting in Ann Arbor.

The custom operations review looked at the following broad categories of service operation, and used the documentation gathered up-front as well as in-person discovery facilitated by the meeting in Ann Arbor to identify service strengths and gaps at a low level of detail. For this reason, further in-depth review of areas found to be in need of improvement may be necessary.

The detailed notes with gaps and action items from the in-person meeting, and gaps identified during the documentation compiling and review phases of discovery were compiled, de-duplicated, and sorted into categories (discussed in Appendix A, Detailed Findings section, below. Compiled data is available in Appendix B). Each de-duplicated item was tracked for the number of mentions it received during the discovery phase, assigned a difficulty and a severity index from 1-5 (where: difficulty of 1 is least difficult, 5 is most; severity of 1 is least severe, 5 is most severe), and then a composite heatmap score was determined using the following formula:

```
score = round(frequency x severity x (1/difficulty), 1)
```

When sorted by highest heatmap score to lowest, this produced a relative ranking of items to address in descending order of heatmap score, thus highlighting the most critical, most frequently mentioned and easiest to achieve issues at the top of the list, with least critical, least frequently mentioned and hardest to achieve issues at the bottom. Issues under each Detailed Finding in this report are addressed in descending order of score, where appropriate. For the purposes of report formatting and strategic planning (natural alignment), some items were coalesced into single topics in the report.

DESIRED STATE, GAPS AND REMEDIES

There are three key factors that lead to the successful operation of any scalable IT service: Data which support the high-level decision-making and day-to-day operational support of the service; the right mix and number of people with the right skills and knowledge to lead, manage and operate the service; and a funding model which allows management to adequately resource the operation of the service. This section of the report is a high-level narrative about two categories of risk to the operation of InCommon services, supported by the detailed findings and associated gaps noted in the appendices. These risk categories are:

1. Short-term risks associated with operation of InCommon services in a steady state (i.e. operating the existing Federation and Certificate services without any major changes, and with no new services and only minor operational changes required). Operating in a steady state under our current growth pattern is unsustainable.

2. Long-term risks associated with scaling InCommon to accommodate new classes of service delivery, new services, and new types of participation in those services. This type of risk is expected to play a prominent role in InCommon's future, with the advent of

new types of support required by the community, including the operation of services associated with TIER.

In order to address the gaps that require additional skills and increased depth of support by people, we need good data to be able to assess not only the gaps in skills and numbers of people, but most crucially to have insight into current service delivery gaps, trends, and success. InCommon is currently not in a position to be able to collect and accurately measure service delivery using data due to a lack of formalized service delivery tools and processes.

To set a direction for InCommon, we need to establish a desired state. We'll start with InCommon's mission statement, from the web site:

> *"The mission of InCommon is to create and support a common trust framework for U.S. education and research. This includes trustworthy shared management of access to on-line resources in support of education and research in the United States. To achieve its mission, InCommon will facilitate development of a community-based common trust fabric sufficient to enable participants to make appropriate decisions about the release of identity information and the control of access to protected online resources. InCommon is intended to enable production-level end-user access to a wide variety of protected resources."*

The mission statement makes our goal clear: provide highly reliable, scalable, mission-critical, secure and trustworthy infrastructure to support the real-time exchange of identity information for U.S. education and research. Recently, this scope has started to expand with the inclusion of eduGAIN and interfederation in the service delivery requirements. With the addition of increased K12 and community college participation as part of the scaling of operations to include regional support consortia, this scope will continue to broaden.

InCommon management must have the right data at its disposal to be able to appropriately resource this change in scope. It must have this data to be able to make decisions to ensure that services are delivered in a way that meets these basic requirements today:

1. Security/trustworthiness
2. Availability
3. Timely servicing of support requests
4. Adequate management of change, including communication with the community
5. Agile assessment of new and changing requirements, prioritization of implementation, and timely implementation according to these priorities

The gaps noted in detail in Appendix A: Detailed Findings, prevent an accurate assessment of whether or not InCommon is meeting basic expectations in these areas. Our best indication that we may be meeting some of these requirements is that adoption of the service remains strong, and that there have been no recent obvious crises in service delivery. As such, we are unable to make an accurate assessment of how to appropriately resource operations in order to meet the future needs of the community.

We must address these gaps in service delivery first, and use the data collected to embark on a path of continuous improvement. In order to collect accurate data about service support, it is crucial that we adopt a service delivery framework such as ITIL or ISO 20000. We need to be careful to adopt this type of framework in a methodical and right-fit way, resourcing the adoption appropriately as we proceed.

The first step on this road to adoption of a service delivery framework is to transition service support for InCommon from the use of mailing lists, which do not allow the collection of service tracking information, to a ticketing or service management tool.

Recommendation 1: Adopt ServiceNow (being considered for adoption by Internet2 Network Services). Examine the need to add additional resources to support adoption of this tool in both the technical and service management areas. Dedicate staff time across InCommon to training and adoption of the tool. Additional staff resources may be necessary to accommodate increased workload. Define metrics and measures that will provide service insight based on data available in the tool and develop regular reports on these measures that will establish trends and provide further insight. Conduct further service reviews based on gaps highlighted by the data, and iterate.

Once data about service delivery is in place, we can begin to determine baselines for service delivery, and work to develop Service Level Agreements which should be published on the InCommon web site and made widely known. This will also lead to the need to set Operating Level Agreements between InCommon operations, Internet2 Technical Services Group, and Network Services, which support the technical infrastructure upon which InCommon operates. This will likely require some normalization of process across Internet2, and may naturally lead to the increased adoption of ISO 20000 within Internet2.

Recommendation 2: Set SLAs and OLAs, measure service delivery against them, and address service delivery gaps highlighted by any excursions from the requirements.

InCommon services depend on a suite of custom software which has largely been developed, and is entirely supported, by Internet2 staff. One area where we know, definitively, that we have a gap in people needed to ensure both current operation of services, and continued growth and change of service portfolios, is software development and devops. Even lacking service delivery data, we can say this for certain because there is only 1/3 of one FTE employee supporting a suite of software and scripts which form the backbone of the InCommon Federation. This is national trust and security infrastructure. It's about to become international trust and security infrastructure. 1/3 of one developer's time is not adequate to provide the depth of skill and level of backup required to deliver this type of service.

For reference, a peer federation, the Australian Access Federation, has four full-time developers currently supporting their (much smaller) federation, and is actively hiring two additional developers.

> **Recommendation 3:** Immediately determine the skills necessary to support the existing software (and likely future development) which supports InCommon operations and the number of FTEs needed to provide for its ongoing, reliable support, and to transition it to a state which will ensure its continued viability and scalable development to meet current and future needs. Determine an appropriate home for this new staff and hire into this/these position(s). Work with current developer to build depth and augment support for, or transition support for, this software to the new hires. Re-assess the adequacy of this hiring and support within one calendar year of hiring.

One area where a significant risk to current and future service delivery was clearly highlighted in the course of the operations review in-person session, was onboarding of new InCommon participants. The existing onboarding processes, which establish institutional identity, bind an accountable person at that institution to the InCommon participation, and set up the technical contact(s) which will be responsible for day-to-day operations of the institution in the context of the Federation and Certificate Services, were designed 10 years ago. In addition, metadata validation processes have also been established for the assurance of endpoints, domains, and other SAML elements. These processes are highly critical to the basic level of trust that participants have in each other via the fabric of InCommon trust services. These processes have been maintained and adapted over the years to address new requirements and changing participation dynamics. However, they are highly manual, labor intensive, and are no longer possible to execute efficiently given the growth of the Federation, the shifting technology landscape and challenges posed by, for example, the anonymization of DNS registration records. The careful analysis and streamlining of these processes should result in more rapid, repeatable, reliable, transparent onboarding, as well as a savings of valuable support staff time which can then be dedicated to other components of continuous service delivery improvement.

Recommendation 4: Assign knowledgeable staff, led by the Director of Technology and Strategy, and including the Operations Manager and Service Management lead, to enumerate gaps in the current onboarding processes, document the required levels of and characteristics of trust established by the processes, and recommend optimizations of processes, procedures, tools, and roles involved with onboarding. This report should be examined by the InCommon TAC and Internet2 Trust and Identity leadership, and the recommendations acted upon in a timely manner.

Fundamental to the trust and security that InCommon supports are secure and risk-appropriate IT infrastructure decisions. In order to establish a degree of independent assessment and peer review in the security practices in place in InCommon operations and its underlying infrastructure, there is a need to directly involve IT security professionals within Internet2 in security-related decision making.

Recommendation 5: Internet2 should appoint one or more members of the new Chief Information Security Officer (CISO) staff as security representatives for InCommon. This/these staff members should conduct a detailed audit of the security of InCommon operations, and the technical infrastructure which supports it, and create a report containing detailed gaps and recommended courses of action. This staff should also be involved in future assessment of IT security as it relates to new and modified InCommon services, on an ongoing basis.

Further service normalization and adoption of Change Management and Service Lifecycle activities naturally support the achievement of continuous process improvement highlighted in the other recommendations. As more data becomes available to make decisions, and the operation of InCommon services matures, the establishment of change advisory and other formal service management structures, as well as the adoption of a service management lifecycle (discovery, prioritization, planning, implementation, operation and governance, and service end-of-life) are necessary to ensure the continued quality operation of services.

Recommendation 6: InCommon should continue to adopt lightweight change management and service lifecycle activities, driven by regular service evaluations of each service component on regular, scheduled intervals. Recommendations for major changes, new services, and service or component retirement should be brought to a change advisory board and that board should manage the planning of and communication about needed changes.

InCommon has undergone a number of structural and staffing changes since the last time DR-BC plans were revised. A number of sensitive and critical DR-BC plans are in place which should be revisited in light of these changes.

> **Recommendation 7:** In coordination with the recommendations above, InCommon staff should revise and expand on existing DR-BC plans, including access control lists for safes and safe deposit boxes which hold sensitive operational material.

As made clear by the recommendations above, InCommon is in need of additional resources, and a sustainable funding model to allow the addition of those resources. Current levels of service operation cannot be maintained without addressing this critical issue. There are a number of additional findings (detailed in Appendix A: Detailed Findings) which are not immediately addressed by the above major findings and recommendations. InCommon should develop a plan, in alignment with the recommended adoption of a service management framework, to continue to evaluate and improve its operations, and to address remaining gaps from this report (as well as new findings which will emerge as a result of the ongoing service process improvement plan) over time. InCommon operations should regularly report on this progress in quarterly reports to InCommon leadership, including Internet2 staff, the InCommon TAC, and InCommon Steering. All of these groups have a hand in the continued success of InCommon, and should act accordingly with the findings of these continued reports.