

CyDentity Sandpit



Homeland
Security

Science and Technology

CYBER IDENTITY (CYDENTITY) SANDPIT MEETING REPORT

June 30-July 1, 2015

HOSTED BY:

THE COMMAND, CONTROL, AND
INTEROPERABILITY CENTER OF
EXCELLENCE (CCICADA)
AT RUTGERS UNIVERSITY



SPONSORED BY:

U.S. DEPARTMENT OF HOMELAND
SECURITY
SCIENCE AND TECHNOLOGY
DIRECTORATE
CYBER SECURITY DIVISION



Homeland
Security

Science and Technology

Report Authors:

Emily Saulsgiver, Tech Op Solutions International, Inc.

Ryan Whytlaw, Rutgers University

Charlie File, Rutgers University

Jonathan Bullinger, Rutgers University

THIS REPORT WAS PREPARED BY TECH OP SOLUTIONS INTERNATIONAL, INC. AND THE CCICADA CENTER OF EXCELLENCE THROUGH THE SPONSORSHIP OF THE U.S. DEPARTMENT OF HOMELAND SECURITY (DHS) SCIENCE AND TECHNOLOGY DIRECTORATE (S&T) CYBER SECURITY DIVISION (CSD).



CONTENTS

Executive Summary	1
Background and Introduction	5
Day 1 Welcome and Opening Remarks	5
Welcome from Director of CCICADA	5
Opening Remarks from DHS S&T	6
Meeting Purpose and Objectives	6
Introduction to the IDAM Engine	7
Provocateur Panel.....	7
Andrew Nash.....	7
Ian Glazer.....	8
Steve Wilson	9
Provocateur Panel Discussion	10
CyDentity Breakout Groups.....	11
Theme 1: Identity Proofing in the Era of Social Media and Data Breaches	11
Theme 1 Breakout Group: Report Out.....	13
Theme 2: Provenance for the “Internet of Things”	13
Theme 2 Breakout Group: report Out	17
Theme 3: Metrics of Trust	17
Theme 3: Breakout Group Report out.....	20
Luncheon Presentation	20
Research and Development Concept Generation	22
Provocateur Panel 2: Insights from the Day.....	23
Concept Refinement and Group Canvassing.....	24
Day 2 Opening Remarks and Concept Presentations	24
CyDentity Sandpit Concepts	25
Next Steps.....	27
Appendix A: CyDentity Sandpit Agenda.....	i
Appendix B: Participant Short Bios	iii
CyDentity Project Team	iii
Provocateurs and Luncheon Speaker.....	iv
Participants.....	v
Appendix C: CyDentity Sandpit Final Concept Templates.....	x
Appendix D: Feedback and Lessons Learned.....	xl

Figure 1: Dennis Egan, Fred Roberts, Anil John, and Doug Maughan review the CyDentity Concepts at the end of day 1.

Photo Credit: Emily Saulsgiver..... 1

Figure 2: Throughout the CyDentity Sandpit, the facilitator encouraged participants to move around, to experience the subject matter in different ways. *Photo credit: James Wojtowicz* 5

Figure 3: The CyDentity Sandpit was hosted by CCICADA at the CoRE Building, Rutgers University. <i>Photo credit: Emily Saulsgiver</i>	6
Figure 4: Joseph Kielman provides an overview of the problems DHS is concerned with when people and systems interact in unknown and unreliable ways. <i>Photo credit: Walter Morris</i>	6
Figure 5: Andrew Nash discusses differences between trust attributes and expectations of consumers. <i>Photo credit: Walter Morris</i>	8
Figure 6: Ian Glazer discusses changes needed in identity systems and training. <i>Photo credit: Walter Morris</i>	9
Figure 7: Steve Wilson discusses complexities within identity and what is and is not working for identity research. <i>Photo credit: Walter Morris</i>	9
Figure 8: Kaliya leads the breakout group in a discussion of identity proofing in digital environments. <i>Photo credit: Emily Saulsgiver</i>	12
Figure 9: Dave Thurman of PNNL moderates a discussion on provenance and the internet of things. <i>Photo credit: Emily Saulsgiver</i>	15
Figure 10: Group discussion on the development of Metrics for Trust in a digital environment. <i>Photo credit: Emily Saulsgiver</i>	19
Figure 11: To inspire creative thinking of the Sandpit participants, Nina Fefferman and Emily Saulsgiver teamed to some storytelling and graphic facilitation during the lunch hour. <i>Photo credit: James Wojtowicz</i>	21
Figure 12: Concept Template and Feedback Form to be completed by CyDentity Participants	22
Figure 13: Small groups formed to develop research concepts. <i>Photo credit: James Wojtowicz</i>	22
Figure 14: Wilson, Nash, and Glazer offer feedback on the draft CyDentity templates. <i>Photo credit: James Wojtowicz</i>	23
Figure 15: Canvassing of Participant Concepts. <i>Photo credit: Emily Saulsgiver</i>	24
Table 1: Final List of CyDentity Concepts	2
Table 2: Overview of the Homeland Security Enterprise.....	7

EXECUTIVE SUMMARY

The ever-expanding internet - with its ever-increasing interconnectedness of digital communities, activities, and interactions - introduces new challenges to securing critical infrastructures, networks, data, applications, as well as individual access from cyber threats, attacks, and misuse. Fraud, terrorism, criminal activities, and hacking can compromise the digital world at multiple levels, from the individual device or computer to network nodes to database or application servers to entire critical cyberinfrastructures. At the same time, the number of smart devices that are networked (i.e. phones or tablets, health monitors like the Fitbit, the Apple Watch, and even artificial organs), and the amount of very private data that is available from them continues to explode. Similar to how the Internet was not designed or built with an identity and security layer, these new devices and the software operating them were designed for simplicity and speed rather than security.

The Cyber Identity (CyDentity) Sandpit aimed to address these challenges by considering how identity, provenance, fraud analytics and network security, in very broad terms, can be combined in a process that would secure cyber and critical infrastructure networks. The CyDentity Sandpit sought to propose and evaluate new techniques that could complement current protection---focused cybersecurity measures being investigated in most U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD) projects. This exploratory activity was designed to develop various approaches for demonstrating a so-called CyDentity concept. The results include proposed alternate concepts to cybersecurity from the author teams formed during the CyDentity Sandpit, high-level alignment of the developed concepts to the areas of competency (authentication, risk, data and application security, access control, and user experience) outlined by the Identity and Access Management (IDAM) Technology Engine, and documentation of these findings in a final report.

The CyDentity Sandpit expanded provenance, trust metrics, and identity proofing in a high-precision process to address secure cyber and critical infrastructures. Participants began by exploring the following three themes. Theme descriptions and key questions, found in the body of this report, were provided to participants ahead of the Sandpit as read-ahead materials.

Theme 1: Identity Proofing in the Era of Social Media and Data Breaches

Theme 2: Provenance for the "Internet of Things"

Theme 3: Metrics for Trust

Over the course of the day and a half, participants developed concepts for research and development (R&D) to address the challenges within the themes and the broader identity field. Table 1 contains the final list of the concepts developed by the end of the Sandpit for consideration by DHS S&T. This table indicates where each aligns with the CyDentity Themes and the IDAM Engine Competency Areas. Author teams self-aligned to the CyDentity Theme areas or an "other" category. The CyDentity Project Team aligned the concepts to the IDAM Areas of Competency, with concepts free to align to up to two areas.



Figure 1: Dennis Egan, Fred Roberts, Anil John, and Doug Maughan review the CyDentity Concepts at the end of Day 1. Photo Credit: Emily Saulsgiver

Table 1: Final List of CyDentityConcepts.

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: 1:1 D Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access Control	User Experience	Other
1	Analytical Approaches for Understanding Risk, Benefits, and Trust Relationships			X	X		X				
2	Distributed Evaluation / Estimation of Trust	X	X	X			X				
3	Social Things: Self-Organizing Networks of Trust for the IoT		X				X				
4	Free Market Economy Based Attribution of Cyber Risk Exposures			X			X				
5	Catapulting Law Enforcement Investigations into the World of Cybercrime	X			X		X				
6	Bootstrapping Identity	X	X	X		X	X				
7	Limited Liability Persona: Bringing the Concept to Life	X		X			X				
8	Allowable Statements Using Metrics of Trust			X			X				
9	Identity Oracle: Proofing/Authentication against one's own behavior, biometric and other data	X				X					
10	Multi-Model Behavior Confidence Measurement for Identity Proofing	X		X		X	X				
11	Smartcard Technology to be used in Drivers Licenses: cost benefit assessment to society	X	X	X		X					
12	Transparency of Federation Hubs			X	X	X			X		

13	Identity Management in Support of Telecommunications Services Authorization for Emergency Communications	X	X			X			X		
14	Identity for Access to Critical Communications during Crisis				X	X			X		
15	Short Text Proactive Authentication	X	X			X					
16	Enabling Social Media Consumers to Understand Privacy Risks	X					X			X	
17	Transaction History of Trusted 3rd Party / Intermediate Operations		X	X				X		X	
18	A Visual Analytic Approach for Analysis and Response to NAT and IoT Attacks		X					X		X	
19	Digital Transformation Innovation Laboratory	X	X	X	X						X
20	Landscapes and Field Guides: Sense Making for Collaboration and Projects Research									X	X
21	Digital Torn Dollar	X		X	X			X			
22	Context, History, Power, Trust of Cyberspace	X	X		X						X
23	Intersecting Realms of Adaptive Provenance		X					X			
24	Combined with 15										
25	Blinded 3rd Party (Federation Hub)			X	X			X			X
26	Leveraging Federation Hubs for Non-Web		X					X			
27	Augmented Trusted 3rd Party with Security Notifications	X		X				X			
28	Personal Management in the Wild				X	X					

29	Global Survey of State to Citizen ID (eID) systems: a comparative eID open source research project			X	X						X
30	How does Nature do “Identity”? Applying Biomimicry to Key Concepts of Trust, Authentication, and Security				X						X
	Totals:	14	12	15	11	9	10	7	3	4	6
		Theme 1: 1:1 ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access Control	User Experience	Other

Following the outputs of the CyDentity Sandpit, the IDAM Engine and CSD will engage the homeland security enterprise and key stakeholders of R&D in this space to prioritize concepts for R&D funding.

BACKGROUND AND INTRODUCTION

Participants of the CyDentity Sandpit were selected to ensure the discussions represented a multitude of perspectives. Academic and national laboratory researchers, homeland security practitioners, international partners, and U.S. Federal government representatives contributed to the Sandpit discussions and activities. Appendix B: Participant Short Bios provides more detail on each of the participants. A total of 40 participants came together for the CyDentity Sandpit. Participants were encouraged to meet people of different backgrounds to help identify where different areas of research and the appropriate expertise should collaborate to help solve problems within the three themes identified for the Sandpit.

Participant Type	Number
Academic	16
U.S. Federal	7
State/Local	1
Industry	10
International Government	2
National Lab	4
Total	40

The design of the meeting was also crucial to the event's success. The CyDentity Sandpit project team from CSD and CCICADA wanted the environment to be creative, the discussions to be innovative, and the outputs to be impactful. To accomplish this, a number of methods were implemented to ensure participants were talking to each other, leaning on other expertise when crafting their research concepts, and looking at the challenges in new and different ways. The CyDentity Sandpit project team leaned on the meeting facilitator, Emily Saulsgiver, to ensure these methods were executed effectively throughout the 1.5 days of the meeting.



Figure 2: Throughout the CyDentity Sandpit, the facilitator encouraged participants to move around, to experience the subject matter in different ways. In this exercise, Emily Saulsgiver explained a study where participants in the study performed better if they stood like a super hero for five minutes before performing a task. *Photo credit: James Wojtowicz.*

For six months ahead of the Sandpit itself, the CyDentity Sandpit project team – made up of Joseph Kielman (DHS S&T CSD), Anil John (DHS S&T CSD), Dennis Egan (Rutgers University) and Emily Saulsgiver (Tech Op Solutions) – met regularly to ensure the meeting design, agenda, communications materials, and logistics were coming together appropriately to achieve the sandpit goals and objectives. The project team also met virtually through video conferences and telecoms with the CyDentity Provocateurs, breakout group moderators, knowledge agents, and luncheon speaker to ensure they were well prepared for the event.

DAY 1 WELCOME AND OPENING REMARKS

WELCOME FROM DIRECTOR OF CCICADA

Fred Roberts, PhD, Director, CCICADA, Rutgers University

The Command, Control, and Interoperability Center for Advanced Data Analytics (CCICADA) is in its 7th year as a DHS Center of Excellence (CoE). Rutgers University is the lead for CCICADA, but 17 other university and industry partner institutions make up the CoE. CCICADA research uses advanced data analysis and computational systems to address natural and manmade threats to the safety of the U.S.

CCICADA enjoys bringing diverse perspectives together to solve homeland security issues. Over the last decade, the team at CCICADA has worked with the U.S. Coast Guard, State and local law enforcement, the FBI, S&T, and other Components to apply computational science techniques and technologies to the really hard problems facing our country. The CyDentity Sandpit gives us another opportunity to help S&T engage in research that will really matter to the homeland security enterprise and the American people, this time in the area of cyberidentity.



Figure 3: The CyDentity Sandpit was hosted by CCICADA at the CoRE Building, Rutgers University. *Photo credit: Emily Saulsgiver.*

OPENING REMARKS FROM DHS S&T

Douglas Maughan, PhD, Cyber Security Division, DHS S&T

DHS S&T CSD is focused on transitioning ideas, including creative new ideas in an effort to deliver outcomes to the marketplace. DHS has also established a dozen international relationships, bringing in \$7 million from its partners to support S&T efforts. The agency is looking to fund work that impacts real infrastructure, an example of which is the new Next Generation Cyber Infrastructure Apex program, focused on the financial sector and routing security. CSD is also funding research infrastructure (e.g. data repositories and network and systems security). Additionally, the fastest growing field within CSD is law enforcement support, and there is an aggressive program focused on transitioning methods (workshops) as a way to engage community and solicit ideas.

MEETING PURPOSE AND OBJECTIVES

Joseph Kielman, PhD, Cyber Security Division, DHS S&T

Cyber identity is a way to approach the problems encountered when interacting with people and systems we are not certain we know and that may be unreliable. There are questions about how this works in a world in which management is decentralized and humans are risk-takers that want to survive. The issue is multifaceted and complex. In this sandpit, we want to constrain the discussion to three themes: identity proofing, provenance and metrics of trust. If humans are



Figure 4: Joseph Kielman provides an overview of the problems DHS is concerned with when people and systems interact in unknown and unreliable ways. *Photo credit: Walter Morris.*

taking risks every time they interact, we need to know what to expect and what we are doing. Is there a way to determine one interaction is more trustworthy than another? We will use the sandpit to gather ideas and to capture perspectives on how to address these problems. The main objectives of the CyDentity Sandpit are to Identify challenge areas within Cyber Identity – identity proofing, securing things, reacting to adverse incidents and metrics for trust – and ascertain research disciplines needed to address these challenges; develop multi-disciplinary project proposals through breakout session discussions and researcher sidebars; and, develop a meeting report outlining the execution process, discussions, and outcomes of the Sandpit. The results of this sandpit will be used by DHS S&T to target future investments in cyber identity related technologies and techniques.

INTRODUCTION TO THE IDAM ENGINE

Anil John, Cyber Security Division, DHS S&T

DHS S&T has launched Technology Engines to provide richer technical support to identity, privacy and data security initiatives in support of the DHS S&T Apex programs and the homeland security enterprise (HSE). CSD leads the Identity and Access Management Engine (IDAM-E) that provides subject matter expertise, analysis of alternatives, workshops, technology mapping services and access to operational testbeds in areas of identity, privacy and data security research.

IDAM-E seeks to help the HSE navigate to identity solutions via stakeholder engagement and high priority problem identification in order to make R&D investments and conduct research projects to address HSE needs.

The IDAM-E is focused on five Areas of Competency and R&D:

- 1. **Authentication** of people and non-person entities
- 2. **Risk** based confirmation of **identity** that leads to **trust**
- 3. **Data and application security** at rest and in transit
- 4. **Access control** at the point of need
- 5. **User experience** that incorporates security, privacy and informed consent

Table 2: Overview of the Homeland Security Enterprise.

Homeland security is a widely distributed and diverse national enterprise.	
The term enterprise refers to the collective efforts and shared responsibilities of those involved in maintaining critical homeland security capabilities.	
DHS S&T considers the HSE and our international partners as our constituency- those we work with and for-to enhance our nation's security and resiliency.	
DHS Components and Staff	First Responders
Federal Partnerships/the Interagency	International Community
Industry	Academia
Private Citizens	Critical Infrastructure Owners & Operators

The IDAM-E will use the results of this sandpit as input into identifying areas of research that need to be funded to meet the needs of the HSE.

PROVOCATUER PANEL

The CyDentity Provocateurs were invited to provide provocative ideas to the participants of the sandpit. They are experts in the identity field, with extensive experience as industry analysts as well as operational expertise in firms with huge identity management and access activities and responsibilities. Each Provocateur was given 10-15 minutes to talk through aspects of identity technologies that are successful and areas that need more help from the research and development community.

ANDREW NASH

A challenge to the group is that everyone in the room believes they know what identity is and what they are talking about but each person likely has a different definition. Non-repudiation, for example, is the question of how do you know a

transaction was completed by the people you think did it. It is broken into three categories but no one cares anymore. At one point in time, however, it was one of the most important issues in identity management. All the time and energy the industry has spent on levels of authentication and terms of conditions has missed the fundamental point that businesses have been thriving for years without such requirements. We have come to a set of expectations that are largely false. For example, PayPal only reached LOA2 provider in the NIST LOA model but operated successfully using basic authentication techniques. If an organization can operate outside of the model, the model is wrong. In essence, PayPal took “stupid” level stuff like passwords and applied risk-based solutions on top of it.

In a consumer world, the most important issue is friction. If you cannot make the system user-friendly, customers will not come back. For example, Google tried changing its sign in process and received backlash. Therefore, identity authority must be hidden and not emphasized or expect consumers to receive training on how to operate. To the consumer, trust is about brand and not about whether an entity supplies good privacy. This is because human behavior is different than what people say.



Figure 5: Andrew Nash discusses differences between trust attributes and expectations of consumers. Photo credit: Walter Morris.

A person may be able to create an identity within six months with a credit rating of 850 and six credit cards with the knowledge of how an identity is created for an individual. It occurs when the first application for credit occurs. Additionally, companies like Experian show only about 60% accuracy with no need to change it. So, what if you presented authoritatively your attributes? Do you need to write an authentication process (yes) but maybe instead of needing to know everything about you, there is an alternative way to think about this?

As we consider attributes or identity context in this forum, be careful, as they can be a slippery slope. For example, a verified phone number has several definitions all with meaning and purposes but all different to different entities. The meaning of attributes is a problem in this area.

IAN GLAZER

There are things that do not work in the identity world. Over the years, we have made certain behaviors habitual of systems users, but we have not effectively trained the masses. Comparability of Devices is another area that is not working. The way device identities are created is mostly proprietary and therefore we are unsure of how unique the identities truly are. Then there is comparability of knowledge based authentication. By commercializing it, it is also proprietary. Further, it requires advanced skills and knowledge including math turning it into a territorial aspect. Overall, we want to ask, “What should I share with you so you have a better informed decision?” But, there is a need to turn the information into something comprehensible.

The identity community leaned on Laplace’s Demon for many years, to include guest lists, least privilege, access control, etc. Overall it states if you know the identity of everything then nothing would be uncertain. It is provably wrong. In non-Laplacian Identity, a person will never know in advance who will show up (the subject), the resources needed (object), or the nature of the interactions (verb). (Subject + Object + Verb = Access Control Matrix) The problem is we do not know the pieces of the equation, so none of the examples work.

However, we could use lots of little things to add up to a big thing by establishing metrics of trust through lots of little less trusted things. This could be done through aggregation but we do not know how to compare those device identities or how strong the authentication occurs on those devices to compare those things. Additionally, there are a bunch of individuals who have been trained to do the wrong things. If we cannot solve these issues we, as a community, are stuck.



Figure 6: Ian Glazer discusses changes needed in identity systems and training. *Photo credit: Walter Morris.*

STEVE WILSON

We as a community should start thinking ecologically about identity and tackle it in biological sense. We need to generalize that (a) the relying party is different than provider party and (b) the user has no prior relationship with relying party. (It is like walking into store that does not take an AmEx card and trying to using the AmEx card.) The merchant doesn't need to know anything other than card number), (c) the user's client knows the relying party, and (d) the user has tangible choice of IDs and ID providers.

The issue of privacy has come up over the years as technology has advanced. Apple Watch and Google Glass have become technologies that gather data. Some larger businesses have tried to determine which customers are pregnant based on their spending habits to encourage that customer to shop at their venues during pregnancy and the first year of the child's life. Other technologies include applications that can provide identification of strangers through facial recognition. In all, some may consider this somewhat creepy while others are not worried about it at all. Privacy versus security is a zero sum gain. The biggest tradeoff is new revenue to businesses. For example, it was recently found that Uber collects data on users after a ride is completed. Some people were upset about this, as it was perceived as a violation of privacy. However, the question becomes whether or not collecting that data may limit uses of that data for new revenue, because then the legal and regulatory game changes.



Figure 7: Steve Wilson discusses complexities within identity and what is and is not working for identity research. *Photo credit: Walter Morris.*

As we address these challenges, here are some things that are not working: high-end federation, LOA - the reality is the risk is not categorized in ranges (e.g. 1-4) but is either yes or no, the privacy debate and, privacy by design that is collecting data for one reason and using it for another.

For some good news, here are some things that are working, however: attributes, FIDO Alliance, hardware security, and data privacy laws that are successful and have been established in 110 countries. For example, Google street view was collecting WiFi transactions along various streets in Europe. Within six weeks of becoming known, a decision was made it was in breach of the law. Some jurisdictions however, are slow to react. Finally, NIST is also doing some good work in privacy engineering as an informatics problem.

PROVOCATEUR PANEL DISCUSSION

Following the presentations of Andrew Nash, Ian Glazer, and Steve Wilson, the CyDentity participants were invited to ask questions of the Provocateur Panelists.

Are you talking about the identity of a person or an entity like the IRS? Should they be handled differently?

That's the point. Each person in this space has different definitions.

I think the issues of identity and privacy are different. Should we decide on which one were talking about?

We have been treating the two items separately and it hasn't been successful. That's how we arrived at current state where we're having conversations about how they relate, and the people who have to deal with the systems are making informed choices.

One thing crypto-researchers and others look for are starting points where we want yes/no answers, but that has failed schematically, and therefore, we need to reset to risk evaluation and the likelihood of success as opposed to yes/no. We want that and it's a challenge.

We talked about how privacy laws are working and the fact that they are working. Would the nationalization of the internet result in consumers relying on nation's laws to protect their privacy for various reasons as countries seek to control their borders? We have already lived through the golden age of the internet.

Don't feel the need to rush to judge how this works out. Legal challenges about borders are important but not novel. Privacy is something so many nations are converging on.

Identity is in the list of things that is not working. What are we trying to do? In particular, in some tasks identity is crucial, such as person to person and others where it's more about risk. We shouldn't narrow the conversation that everything must go through identity. We need a discussion about when is identity the best way but also not always the primary method.

I don't think we can separate identity and privacy. Defined authentication is the task of finding out identity related to what do I need to know about you to be able to do business with you. Privacy is what I do not need to know about you to do business with you. Privacy gives way to security.

We need to understand tradeoffs between the two.

In considering authentication is what we mean by identification an issue. The more interesting question is: Are we dealing with identification?

Can you trust an inanimate object or a place holder for assurance or do you trust the builders?

Consistency of behavior is important. That's how we build trust.

Trust doesn't occur in most transition thought processes.

The term trust doesn't mean the same thing in each example the questioner raised. At what point is identity important and when do you want to trust it? Consumers place brand trust in decisions so what does trust mean?

Trust is important but not sure if it's necessarily the right language.

The presenters have used the term risk but that too means something different.

That's correct as some people consider the things that can affect me and likelihood. Some entities have used risk as part of the formula without understanding what it means.

High risk for one business is different for another.

Financial risk is affected by both systemic and internal impacts.

The discussions are getting at the difficulty in agreeing upon definitions. In pulling back to something presented by Steve on the LOA, there is a lack and need for professionals in technology study of governance. In the past, attempts have been made to group lawyers, engineers and policy experts together with nothing to show. Could you speak more to cross border privacy in terms of whether it's working or not and more to the vectors of trust?

Those who answer one way or the other is pushing an agenda. I think it is working and I'm pushing an agenda. Vectors of trust are important as it acknowledges there are multiple inputs to trusting a transaction. Things are not always binary but in routine transaction it's really simply yes and no. (Whether a credit card is accepted or not is one example.)

CYDENTITY BREAKOUT GROUPS

The CyDentity Sandpit participants were divided into three groups based on their background and experience, to ensure each group had a diversity of perspectives to discuss the theme area. The break out groups were to investigate the concepts within the theme areas so participants could start identifying areas where research and development activities may help address the challenges across cyber identity. Theme descriptions, scenarios, and key questions were provided to the participants ahead of the sandpit.

THEME 1: IDENTITY PROOFING IN THE ERA OF SOCIAL MEDIA AND DATA BREACHES

Moderator: Kaliya, Leola Group

DESCRIPTION: What challenges exist in each of the identity proofing steps with respect to balancing privacy with the need for data collection, ability to validate information when source authorities are not available, and lack of confidence in verification that depends on knowledge based questions which can be answered by mining social media or bought in underground forums that sell data from breaches. Mobility in the era of ubiquitous smart, portable devices, requiring identity proofing anywhere and anytime, further complicates these steps. Furthermore, if the goal is truly real-time functionality, the usability of proofing methods becomes a major concern.

SCENARIO: Anywhere/everywhere, anytime/always-on social media; a constant stream of data breaches; and national ID or identity cards. These are just a few of the aspects of our cyber environment being discussed in national-level conversations.

KEY QUESTIONS:

- To what level does the first topic contribute to the second?
- Is privacy possible or even desirable under such conditions? Or, is it even relevant?
- And would the third topic be a realistic way to mitigate the potential damage caused by the second?
- What should we know about the source or history of data to trust them?
- How do you know you can trust where your data came from or who sent it to you?
- What and how are decisions made regarding privacy within a network and information sharing systems?

GROUP DISCUSSION:

NATIONAL ID VERSUS SOCIAL MEDIA IDENTIFIERS

Identities are provided by different bodies, like a National ID that issued by a governing body versus a social media identifier that is chosen by the user and then confirmed by the social network managing body. Different entities are responsible for issuing and validating different identities and associated profiles, and there are good and nefarious reasons for having multiple personas. The national security perspective is trying to balance trust and privacy. Social media users do not necessarily want their identities in an online environment connected with national IDs, however. How are these boundaries established, maintained, understood, and accepted by different users? There are varying levels of trust and certificates when using different systems and devices to handle one's identity and identifiers. Attributes that describe a user and enable access rights are different in different systems, and if compromised can be given away to enable access to other systems. For example, security questions to affirm your login to one system may be the same questions one would use to get back into a bank account.

SOCIOECONOMIC CHALLENGES WITHIN ID PROOFING

There is also a question of socioeconomic challenges with identity, especially when considering access to public services. If an ID cannot be validated, the government cannot deliver the services an individual or family may need. This becomes a particular concern when dealing with emergencies and crisis situations, emergency assistance and medical aid. How

do you know how to effectively communicate with underserved populations if you do not have enough identifiers to understand their needs (e.g. deaf, homeless, etc.)?

LOCATION AND BEHAVIOR

A sense of one's location may be garnered by revealed identifiers and behaviors. Who controls access to this information? Just how much information is needed to understand where an individual is? More and more systems will enable understanding of location just based off of a user's name.

REPUTATION IN ONLINE DATA BREACH PROTECTION

If a data breach occurs in an online system, how do you know if it's a real breach or a rumor of a breach? What if the source that divulges the breach is unknown or not well known? If no reputation on the entity has been validated, it may turn out to be a false claim which could impact the reputation of the online system. A web of patterns would need to be investigated to authenticate the entities. This requires access to data that is not always accessible. A challenge here becomes who owns the data, who can share it, and under what conditions does sharing and joint analysis take place?

IDENTITY MANAGEMENT FOR DIFFERENT PURPOSES - WHY IDENTITY PROOF AT ALL?

Different systems use identity management for different purposes. Different systems store different credentials and authentication. Identity proofing itself may constrain these efforts. Does your ID build over time or does it keep changing? What are the data limitations over time? On social media, your identity is more a reflection of your memories and experiences. Different scenarios are needed to establish identity. Laws have been established to protect user data, but should all data be distributed or should there be one place to find certain data? There are different tolerances for risk, data, and accuracy, with different consequences. If you have completed a process, for example, why does the system need to hold onto the data? The establishment of an ID should have a limit on data retention. However, retention may mean usability at a future time. It could also just be lax data storage practices that keep everything so the data does not need to be sorted and determined if still relevant.

The usability of identity proofing then includes the contexts of social information and is not trustable at all levels. Facebook information may be more or less useful than getting a user to fill out a form, depending on the identifiers needed to prove ones identity. The user could provide false information in both forms of data collection.

Considering this, is behavior more important than who an entity says they are? Behavior over time appears to be the most important element in most scenarios. How do you proof identity in an era of non-traditional documentation, like cell phone communications and apps? What is ID proofing in such an era? Is it monitoring change in your behavior? Risk scores and behaviors can demonstrate how a system might perceive you as a liability or a trusted entity. However, when looking at this tactic for ID proofing, what are you trying to protect against? What is the expectation of privacy and security around new identities? Are digital, behavioral artifacts more trustworthy than identity proofing techniques? End users tend to do things one way, and thus leave behind their own behavioral trail. However, the users do not have access to that trail, which means the individual is less empowered in the system.

Banks require identity proofing to avoid fraud and theft. Do we just have to deal with these boundaries when working with different systems? Banks in the UK, Australia, and elsewhere now require you to physically enter the bank to open accounts so they may validate the identity of the account owner.

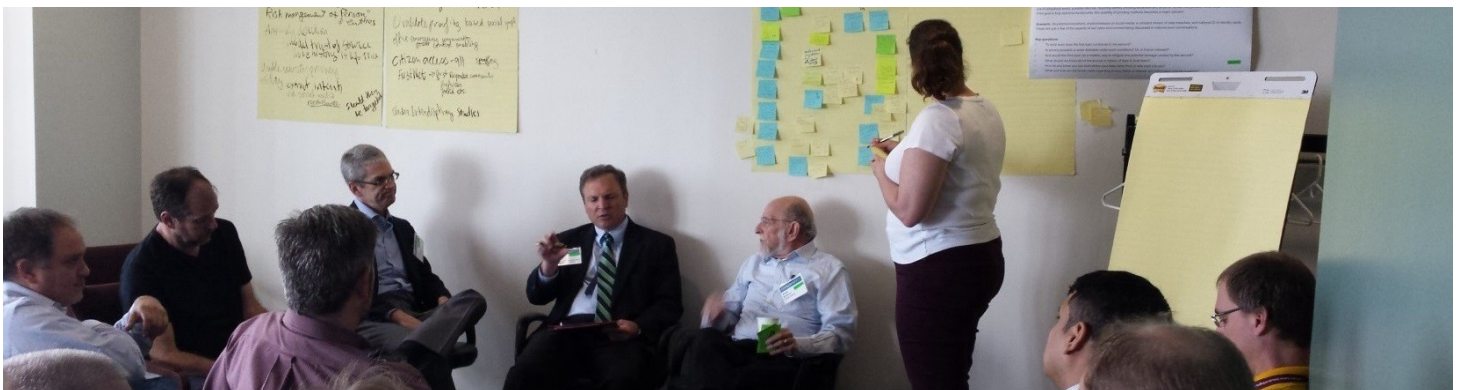


Figure 8: Kaliya leads the breakout group in a discussion of identity proofing in digital environments. *Photo credit: Emily Saulsgiver.*

How is trust aggregated across information sources? How do you understand integrity when trying to counter malicious intent? Can triangulation of linked IDs found in tax systems, banks, etc. ensure identity proofing is accurate? How do we understand how much of this information can be forged? If someone uses a license as a form of ID, do we know it isn't forged? We deal with information that is incorrect all the time. How do we establish general trustworthiness? Multiple forms of ID may be needed to truly proof an identity of an individual.

Scale comes into play, as well, when considering massive attacks and trust of companies, not just individuals. The context of an ID becomes crucial. The risk threshold varies with context.

KEY TAKEAWAYS

The group identified the following key takeaways when considering identity proofing:

- Context
- Behavioral characteristics as validation metrics
- Scale and consequence – individual vs. business, correlations between
- Spoofing of identification
- Limited liability persona
- Privacy selective sharing

THEME 1 BREAKOUT GROUP: REPORT OUT

Kaliya summarized the discussions of the Theme 1 Breakout Group. The main points of discussion for the group included:

- What is ID proofing? Is it even relevant to think about proofing static characteristics? Or is behavior over time more important?
- Goals for Identity Proofing: Prevent spoofing, create an accurate representation, creation of an identity separate from spoofing, limited-liability personas, and the ability to identify someone but not link to all other work/social/family contexts. Is this even possible?
- Conceptuality: National identity influences in identity, the thin file problem: 20% of people showing up to be proofed didn't have enough in their file to be proofed against. Not everyone has set of formal identifiers. How do we help them build identities?
- Scale: Impact on an individual vs. impact on a business vs. attacking whole systems.
- Selective privacy: Choosing what you share and where. How is individual enabled to collect their own behavior data?
- Integrity: Understanding behavior changes as a signal for bad behavior in systems. Correlation as a function of consequence. Understanding risk.

THEME 2: PROVENANCE FOR THE “INTERNET OF THINGS”

Moderator: Dave Thurman, Pacific Northwest National Laboratory

DESCRIPTION: Provenance here refers to a recorded history of a digital object, which captures that object's point of creation and all subsequent transfers and transformations. Provenance must include the actions taken on or with an object and the actors who took them. Today, some type and level of provenance is available for some digital objects. The research challenge is expanding the notion of provenance such that it is universally available to ensure an acceptable level of trust in the identity of the objects.

SCENARIO: Today's critical infrastructures are often controlled by obsolete SCADA systems that were designed and built as closed ecosystems. None were meant to be interconnected nor connected to the chaotic world that is now represented by the Internet of Things.

KEY QUESTIONS:

- What are the threats?
- What challenges do infrastructures owners or providers face in protecting their systems and interconnections?
- How do we build smart cyber defenses useful for dumb Infrastructures?

- How would we then measure the security of an individual component, of a sector's infrastructure, and of the interconnected cyber-physical world?
- What do we protect and to what level and at what cost?
- How can we model individual and societal responses to cyber failures?
- How do people interact and react under various stress conditions?
- What are the interdependencies of infrastructure protection and societal practices?
- At what point does the system break down?
- What can we measure and use as indicators?

GROUP DISCUSSION:

PROVENANCE AS A FUNCTION OF BEHAVIOR

Provenance needs may vary greatly. One may only need to know the last transaction in order to function. It may depend on the type of transaction. Entities may only care about provenance across one transaction, but the manufacturer may want a broader view of all transactions. Provenance may also be based on behaviors not identity of objects. The provenance question then becomes, is this behavioral pattern predictable? What about new behavior? This design would create institutional memory as a provenance based on behavior. How is privacy protected if the system is then analyzing behavior? Provenance would also depend on other factors, such as the context of that behavior. Behavior would not necessarily be connected to identity automatically, but certainly can be based on what, how, and how much information is connected on a user.

INFRASTRUCTURE IDENTIFIERS

Cyber infrastructures have numerous vulnerabilities, some with higher risks than others. This creates severe problems with deployment. Deployment at scale becomes a real issue as it depends on everyone having something in common. With an already populated ecosystem with many different players, how to deploy given heterogeneity of those players? There is no standard way to do discovery of the "thing" (in the context of "Internet of things") because the identifiers are not standardized. Thus, discovery of a "thing" with current techniques and technologies is hard today.

ISO 291195 has protocols for identifying non-person identities, but IoT is not a homogenous environment. The same device can live on multiple networks. When we ask for provenance, we must ask *which* provenance. Artifacts of a home security system all belong to one group, but because they operate on a WiFi network they can talk to other devices on that network. Maybe it's also connected to a cloud computing platform. So, when tell a device to "identify itself," in what context do you mean?

A car, for instance, can have a specific number, but when rented to different people it has different access controls. New apps like Uber can change the identity and behaviors of the car, as well, based on who the passengers are, the purpose of the trip, and where they are going. How much of provenance is transaction-dependent?

LEVELS OF AUTHENTICATION VERSUS PROVENANCE VERSUS SECURITY

When do we care about authentication and we do we not? Why care about behavior? Millions of devices in use had a WiFi link installed at the factory for firmware programming that are now unintentionally part of this network of things, even if they were never intended to have networking capabilities. How do we measure the security of such elements on our networks? If we curtail devices to adhere to current norms and security needs, we may be compromising future capabilities of something we have yet to envision.

There is a tremendous lack of discipline in this space. Manufacturers focus on engineering and customer needs and thus only build what is needed right now without considering possibilities in the future. Why not just pump everything up with computing power and figure it out later? Of course this is difficult in the security context because we need to know where we are going in order to figure how to secure devices once they get there. What does security mean in an environment where users want to build apps into a manufacturer's product space to allow people to program their refrigerators, homes, things of all sorts? In these kinds of use-cases, the use-space is yet to be defined, so security characteristics of the space are not fully defined.

Thus, security criteria need to be modular. For verification, the modules need cooperation structures. They need to have recognitions about how we verify, modular and cross-recognized. There needs to be trust between differing organizations and their credentialing process. At what point do you make security policy decisions about systems of things that are

connected or disconnected in certain ways? This notion, however, undermines the idea of an IoT if some of them are disconnected from the network. This model is something else entirely. Instead, we accept that all these things are going to fail, and then ask, “How then do we deal with that failure?” The perspective that everything must be 100% protected at all times is not feasible. This means one piece cannot be more critical than others. So then, how do we isolate in a failure situation? Using modularization or separation?

For example, on an electrical grid each unit can decide what is normal, and each unit can decide normalcy has been violated and cut itself off from the network. Without knowing the use-case, this can perhaps be solved by using a learned history of the behavior of the entities, and those entities engage in the network as the behavior adheres to normalcy constraints. Then one could see non-normal behavior or un-safe behavior. This allows for new behavior based on a flexible connection and also flexibility for levels of interaction.

ESCAPING SILOS OF INTERACTION

Currently, the model of IoT is what we see today in coffee machines: buy one device, pay for their app, and it may not talk to other brands or devices. Thus there are many different silos of interaction. One value of provenance is to facilitate interaction between devices, to escape this silo model. This is where standards are important. The next level of standardization needs to focus on relationships. For instance, Facebook works not because of self-assertions of identity but because of relationships that create the identity. We can use this metaphor in the context of connected objects. We can rely upon shared links between objects and the individual. These rules also provide the ability to identify new people or new objects.

PROVENANCE OF INTERCONNECTED SYSTEMS

We can try to define provenance as a function of a household network, an amalgamation of devices, as a set of transactions, as a definition of a system (be it a clique of people or regular information exchanges), but these are socially learned norms. These types of systems are constantly in flux and changing and they are fluid. Humans are fine with such fluidity and handle it well. Can we teach our devices this? How does the power grid learn to trust the house? How does the kitchen trust the new fridge?

First responders want to tap into a security or fire suppression system directly at the front door and not have to go to a special room. Current technology allows this; with the right credentials anyone can anyone access fire alarms, occupancy sensors, etc. But this is provisioned today. How will this change in the IoT era? How do they tap into the devices in peoples' houses? How can the system adapt to new scenarios, when new devices are added, when use changes?



Figure 9: Dave Thurman of PNNL moderates a discussion on provenance and the internet of things. *Photo credit: Emily Saulsgiver.*

How things are phrased is a big part of if something is seen as “creepy”. Communicating things correctly to the public is key. It may be that humans need to be in the loop to check that things provenance/authentication systems are working correctly. Again, humans are great at this kind of thing. Will we reach a point where algorithmic decision making becomes good enough that we do not need humans? One way to accomplish this is via anomaly detection, but if these use cases are new, how do we know that though new behavior is happening, we are able to assess if it is bad or not? Even if we can judge a behavior as completely normal (based on moving averages, etc.) can it also be completely bad? How does this scale for the Internet of Things?

Resilience may be the key point. How do things play out if we set up machine learning algorithms to pick up anomalous behavior, and can then apply the label 'wrong' to those behaviors, how do we do this in an environment where these new connections are constantly being formed, how can we establish that this behavior is acceptable without a history of judgments to draw upon now? Who are the bad actors?

There is a fetish for interconnectedness. There won't be preprogrammed connections, but ones that are invented or created on the fly. There are many risks in interconnectedness for its own sake. For instance, though we may trust a person, their device could be hacked. People themselves can be hacked. There are conflicting goals and objectives, as well. What constitutes a "bad actors" is personal to each individual. What we call a "bad act" applies to realm in which it has an effect. In the realm of building security, some systems lock doors, while others open them in the case of a fire. In the future, there may be some smart algorithm that decides what the best thing to do in that instance: to keep them open or to close them. This decision may get people killed, or it may save them. Which system will win, the security system that locks the doors or the fire system that opens them? Why will it win? Based on what rationale? Based on whose judgment? Based on what factors? Algorithms are fundamentally unpredictable? Who is responsible? Who is accountable? We need to have some policies in place beforehand.

One possible answer to this lies in a research area called "salience search." It asks questions like: What do we focus on in various contexts? How do people consider all the ramifications of linking their objects or establishing relationships? We don't have 100 years of fraud monitoring experience. We can't yet draw upon that history like the financial sector does for their machine learning algorithms. But we do have social and economic analogies and metaphors to use in the case of, for instance driving decisions made by the algorithms that control self-driving cars.

In the IoT, people interactions will be a small fraction of overall interactions. The vast majority of transactions will be between objects, so different scales are important. Algorithms can be designed to learn what is normal as an endogenous outcome of observation, rather than needing to define a priority, define what is normal. Thus anomaly detection doesn't require top-down monitoring, but bottom-up observation. For example, people can't define what a normal day is, but if you ask someone if they are having a normal day it's an easy question for them to answer because they are working from observations rather than trying to make universal guidelines. You can't define a normal day for a city, but you can define modular normalcy for different departments like sanitation or police. Any one of them may have anomalies, but overall, averaged across all departments maybe it was a normal day.

This metaphor of the city seems to be a good one. It seems to include notions that have been discussed, including a bottom-up definition of anomaly, emphasis on resilience as important, sense that resilience is fluid and context-dependent, a consideration that what is important in security may change over time, and that things that are anomalous are not necessarily bad. The 911 system is an efficient model of anomaly reporting. Bottom-up and top-down approaches can both provide feedback and hopefully agree on a good middle ground.

SOCIETAL DECISIONS AND FUTURE IMPACT

Provenance of anomalies can vary according to a number of factors. For instance, consider provenance of anomalies of man-made vs. natural disasters. How much we care about this depends on the activity we are undertaking. For an attribution problem we want all the history we can grab. The temptation is to time log every single thing into an endless collection of behavior history so that we have endless amounts of data but it is pointless. We don't actually care about the vast majority of that data.

People can take down an air traffic control system from the Nest thermostat they have installed in the tower. We can take down the power grid from an iPhone. What is the point of keeping track of endless numbers of devices and endless numbers of transactions? How do we input elements of society, culture, norms back into the equation of how we make decisions?

This doesn't have to be a top-down thing. These are all endogenous behaviors of that can be detected as patterns of behavior within the interactions of actors in that system that can be detected in an emergent manner. Societal practice is one way to regulate or guide the evolution of the IoT. Do we need this control so you can't hack an iPhone and take down the power grid? Is that what we want? Or need? Is this something we therefore need to make "secure." For instance, does every FitBit need to be a part of that, does it need to be "secure?" In other words, in a world where every person

can have 5 connected devices on their body and every house could have 50 connected devices in it, is that worthwhile to attempt?

It can be helpful to look ecologically at technology. Ecology is a way of looking at why things are the way they are now and asking how they have gotten to where they are today. We can use this perspective successfully: In the realm of identity verification, it looks like all the IDs in my wallet are the same, so why not use my bank card for health insurance? The answer is that it turns out that identities are siloed. The bank identity, the health insurance identity, etc. each have their own specific needs and requirements. These can be considered identity 'niches' similar to biological niches. Each identity niche has own pressures of business need, privacy need, etc. Different identity 'species' have evolved to fill these particular niches in order to fit to the pressures against them.

Silos may be each unique, but quite often they have a large amount in common, so there may be a great deal that they can share. This is important to recognize. Everything is optimized for the short-term. The question of if, on the long-term, this was the right thing to do, we don't really have an answer for. We move to optimize some set of resources, but we can't predict we go in any certain direction. Does this help us therefore understand how things will move in the future?

THEME 2 BREAKOUT GROUP: REPORT OUT

Dave Thurman summarized the discussions of the Theme 2 Breakout Group. The main points of discussion for the Theme 2 breakout group included:

- A discussion of, "what is provenance; what does it mean from different perspective?"
- Perspectives such as: Manufacturers, Users, Devices
- Can we think of behavior of device as part of its provenance? Are patterns of that behavior is useful?
- IOT and critical infrastructures: an increased vulnerability. IOT needs some shared infrastructure for provenance. There is some information that needs to be shared. Governance should be more a decentralized standard than an oversight organization. There needs to be some way to share information and come to an agreement on risk, infrastructure, etc.
- How do we identify IOT devices? We need to get beyond IP and MAC address. Identity varies based on scale. For instance, a car can be identified as: a vehicle, a device in a vehicle, the driver, or the passengers. This is dependent on the transaction. Need to think about the minimal level of information needed to conduct that transaction.
- Critical infrastructures are very heterogeneous. For this reason, they can't be managed top-down. It is an ecological environment of people and devices that evolves over time. It may be that ecological approaches are helpful.
- Marketing of IOT typically is based on the ability to do anything with them. In order for that to work, security can't constrain the ways they talk to one another. Thinking about security, we need to think about the transactions that need to take place. However, we cannot manage future uses or predict how things will develop.
- Service-oriented infrastructure might provide lessons learned for this topic.
- Is there an algebra to be created that allows one to take some level of security or provenance from some group of subsystems to construct a larger assessment of overall security of the system?
- Social norms: are there lessons to be taken from society about how to govern how devices should interact?
- Devices used in an emergency situation are often used in unintended or unpredictable ways? Can we account for this? Do emergency services want to tap into these devices?
- We want to have humans in the loop. At what point are humans required to evaluate interactions between devices? How do humans oversee all this and how do we avoid information overload?
- Cities are a useful construct or metaphor for IOT. Both evolve and emerge over time. Both have some planning or direction but also some emergent evolution. It may be worth looking at how the development of cities can provide an example of growth, moderation, and management of infrastructures.
- Financial fraud detection uses machine learning that can draw upon fifty years of examples and experience. How do we build models for anomaly detection with no analogous history?

THEME 3: METRICS OF TRUST

Moderator: Dennis Egan, Rutgers University

DESCRIPTION: A third objective for the CyDentity program is to offer a method for quantifying and expressing the relative trust of our cyber infrastructures, digital objects, and cyber identities. Metrics and measurements could be helpful

in specifying the level of security or trust attainable and in making decisions about how to select and allocate cyber defenses effectively. Metrics that involve the degree of expanded provenance and identity proofing attainable might need to be augmented with metrics for expressing the value of the data or information contained on networks.

SCENARIO: Fraud is an ever-present reminder that we as individuals and our computer systems consistently mistake the identity of those individuals or systems with whom and with which we interact. Money or identities are lost; infrastructures are compromised and rendered inoperative; illicit or counterfeit goods are exchanged. We engage in risk-taking behaviors without ever knowing the extent of the risks involved, and without consideration of the potential secondary effects on our communities and social infrastructures.

KEY QUESTIONS:

- Can we use risk as a proxy for trust in such situations?
- What does preventing fraud teach us about security-proofing our cyber systems?
- What types of tools are needed to communicate fraudulent access and activity?
- What does risk mean in a cyber-world?

GROUP DISCUSSION:

To start the discussion, participants of the breakout group took turns discussing ideas for metrics for trust and which problem(s) such metrics would help to solve, such as:

- 1) Reliability and repeatability to measure trust, and the eventual ability to predict reliability.
- 2) Trust as context sensitive: For example, you may trust a person for some things but not others. Also you yourself may have varying levels of trust. A metric of trust should account for this kind of variability.
- 3) Trust should be sector specific, widely adopted and replicated.
- 4) Consistent behavior under surprising situations as a metric for trust. If you try to come up with a test whether a source is trusted or not, we often try to see whether the source is doing what they're supposed to be doing. For example, if the IRS calls, how do you verify if it is a scam or not. You would put them in situations they were not expecting to verify if they behave consistently. We know we can write machine learning that can recognize who you are but what happens if someone invades and steals ID? How can you trust it? For metrics to be valuable, they need to be generalizable.
- 5) Semantic Interoperability: Semantics is a problem in making language understandable. In the theme of trust, this may be developed in three levels "well known", "heard of", and "unknown". How a person may trust something might be different. It is foolish to think the same metric for trust can be applied across the board.
- 6) Established confidence level: In all cases, you would want to be able to quantify the level of confidence in a statement. As an individual, or user, why can't you limit your exposure? How can both end parties contribute their thresholds for risk for the development of a metric? Money provides a universal indicator. May have some correlation to insurance industry where multiple people buy in.
- 7) Reputation is a scarce resource to be used for trust.
- 8) Provenance of access channel. This would look at how a person reached its current point. Can a decision be made based on a person pathway? Can we look at consistency of the transaction (have we seen this elsewhere), or the consistency for groups? This would refer to does an individual make a transaction with group X? Is there value in a centralized context that everyone buys into? Sometimes central hub is good but in some cases it's not. Consistency is better depending on participation. Central hub is not generalizable. Some of the ideas are domain specific. The idea of transactions is not always the area needed for trust. For example, senators stating facts that are not accurate. The question is do I trust this while no transaction takes place.
- 9) Validation of implicit expectation: Matching some external indicator to determine if this is a trusted channel or source. Could we have a means of validation? It seems there is more object of trust. Trust is a human relationship and difficult to quantify. Perception of risk may be different but to me, the purpose of a metric is risk mitigation. For example, at what price am I buying a used car and is the car trustworthy? A \$10K car brings more expectations of trust than a \$3K car. Duality between objectively and subjectively determining trust. Objective is how much but initial relationship is based on reputation which is both subjective and quantifiable. You could take it to a mechanic, a lab, or take the salesman's at his word. The trustworthiness of the salesman is subjective and that's the relationship. But then you could get ground truth.

- 10) Third party assessment: Health rating is a metric of cleanliness which is 3rd party provided with a set of standards the health department goes through. Does that letter grade influence my rating – yes. The decision to go to the restaurant is based on both an individual relationship with a restaurant (personal thoughts on food, cleanliness, atmosphere, etc.) and some metrics related to standards (health inspections). For it to be consumable, it needs to trend more to something that is repeatable. There is value to both reviews. One is about experience and the one whose taste I agree with. The weights of the measures vary by person. There is a trustworthiness that is factual. The purpose of the metric (I believe is objective) is risk mitigation so it depends on being objective.
- 11) Number of independent sources in agreements: I don't trust anyone. Humans in general are evil so assuming that, trust level is low. If there are independent sources (e.g. when buying a car you can test drive, get reviews, listen to how it sounds, looks, and feels) it can build trust for the decision.

PURPOSE OF METRICS

Metrics for trust can be tricky. The purpose of the metric must be understood because with it comes baggage and power. Should a metric be rationalized across boundaries? Trust depends on relationship you're trying to broker. If you make known what is being measured, can the system be gamed? Can we get away from that? How do we evaluate? Can we evaluate truth statements or ask others about it and average/weight it. Bottom line is the need to try and evaluate confidence of something. There is a threshold when making decisions. Relationships help determine the issues based on lots of metrics and statistics. It's not a single episode where things happen once and not again that we worry about. But the issue could be that we did a trust evaluation once of the root CA (Certificate Authority) and never did it again. A risk profile may change and therefore the need to go back and validate and re-measure/test it again. Processes such as this are not how we build relationship in the real world. Humans don't conduct background checks and investigations prior to becoming friends with a person. Having health inspector or physiological work up is not how we build trust as humans. It's different in that going into a restaurant you go in with a level of confidence of cleanliness based on health department ratings.

TERMINOLOGY OF TRUST

Do we really mean trust? Does it have to be something that evolves over time, and re-evaluated. Consistency in some ways addresses reputation or transaction history related to what have you purchased/consumed and how have you purchased/consumed it. We should not be using the words trust or trust worthiness. We need to use terms that are consistent across channels.



Figure 10: Group discussion on the development of Metrics for Trust in a digital environment. Photo credit: Emily Saulsgiver.

RELATIVE TRUST OF CYBER INFRASTRUCTURE AND DIGITAL OBJECTS

One question raised is who do we have more trust in? The system where it shows how often the system is tested in black swan situations. If I'm Secret Service and I'm about to use a system, would I as an agency have more confidence of a metric of trust related to how often do they test the system so they can then trust the system on a regular basis. Then the question would be: what you do about it? TSA has been miserable at finding guns. What they do with it is more interesting. That's the interesting bit there. Two considerations are 1) are you disclosing how to gain confidence and 2) are you solving problems? The stakes/risk is relative too. Are the stakes high when a gun is brought onto a plane? The TSA example is good. There is a proxy that informs individual decision/action: do I not fly because of poor security? This is an individual issue. Consistent inability to do something effects decision.

In reflecting back to the theme description, the conversation has lead heavily towards the individual level. Organizations may want to verify as well. To what end is the purpose of metrics of trust? Is it for the consumer, victims, etc. and is it for individuals, organizations?

The group used the theme description to begin identification of starting points for considering metrics for trust. The group developed a matrix with entities along the x-axis and the metrics of things along the y-axis.

There is a need for ongoing assessment. This will support catching insider attacks. Some in the group disagreed and said insider attacks are not an identity question. Using consistency, insiders can be caught when they act abnormally. The interesting question is addressing false-positives and how to address things that happen the first time and yet do not pose a risk.

THEME 3: BREAKOUT GROUP REPORT OUT

Dennis Egan summarized the discussions of the Theme 3 Breakout Group. The main points of discussion for the Theme 2 breakout groups included:

- Some of the initial characteristics of trust metrics identified were metrics are reliable and repeatable, context sensitive, and useful for different purposes and end points. They should be helpful and understandable to both sides of a transaction. Metrics could reveal consistent behavior under surprising circumstances, and involves semantic interoperability (e.g. easily to understand language). The metrics developed should help the quantification of a truth value of a statement.
- Discussion occurred regarding the potential of trusting a person up to a dollar amount. Is it possible to assess trust or reputation from a network? Reputation and using a dollar amount are similar. There were also some ideas about needing to know something about the provenance of the access channels and the consistency of the transactions which take place there. In some instances, third party verifications through a third party who using a set of standards may be used to measure trust (e.g. using the Better Business Bureau to research a business or bringing a car to a mechanic to assess its quality before purchasing a vehicle).
- Metrics developed should reinforce the idea of a person or thing that has similar values to my own value. The group also mentioned the potential for individuals to game the system of input signals effecting the metric or measurement of trust. (E.g. yelp reviews could be used as a metric of trust but the system can be gamed.) A single measurement isn't good enough and the metrics need to be updated over time.
- To organize the discussion, the group created a matrix. The metrics across the x-axis include third party assessment, consistency of behavior (e.g. putting other side in an unusual situation to see if they respond consistently), notion of reputation in a network, and first party assessment. In addition to looking at how each occurs in each setting (infrastructure, objects, identity and organization) there's a whole bunch of stuff the group did not get to but determined there is a need to figure out bigger issues first. But combining, algorithms, etc. are some of the follow-on activities. Others include, can you probe the other side with a test, update risk appetite, and can you assess the trustworthiness of what you are interacting with? This may be used instead of having someone else make the determination.

	3 rd party assessment	Consistency of behavior	Reputation in a network	1 st party assessment
Infrastructure				
Objects				
Individuals (Humans)				
Organizations				

LUNCHEON PRESENTATION

Dr. Nina Fefferman and Ms. Emily Saulsgiver

Dr. Nina Fefferman and Ms. Emily Saulsgiver teamed up to do a luncheon presentation on the Next Generation Communications Interoperability (NGCI) experiment, conducted by Dr. Fefferman earlier in the summer. While Dr.

Fefferman told the story of how the NGCI live action role playing (LARP) took place over the course of a week, Ms. Saulsgiver drew out the story line on a whiteboard. This activity was intended to encourage the Sandpit participants to think about the relationships, challenges, and research needs concerning the validation and understanding identity in a different way, using a creative approach to describing and communicating the issues using the scenarios explored in the NGCI LARP.

Over the course of the NGCI LARP, two teams sought to win the LARP by finding and assembling puzzle pieces that were hidden around Rutgers' campus. Technically, only one team had to find and assemble the pieces, the other team just had to make sure the first team didn't figure out the message contained in the assembled puzzle. The teams were only allowed to meet in person once a day for dinner and all digital communications were to be shared with the event organizers - dubbed "The Ideological Leader". The teams weren't told they couldn't meet during other times, just that "a safe house" had been reserved for them for dinner. Team members were not told who else was assigned to their team, so they had to vet and validate each new member to ensure they could trust them to help solve the puzzle.

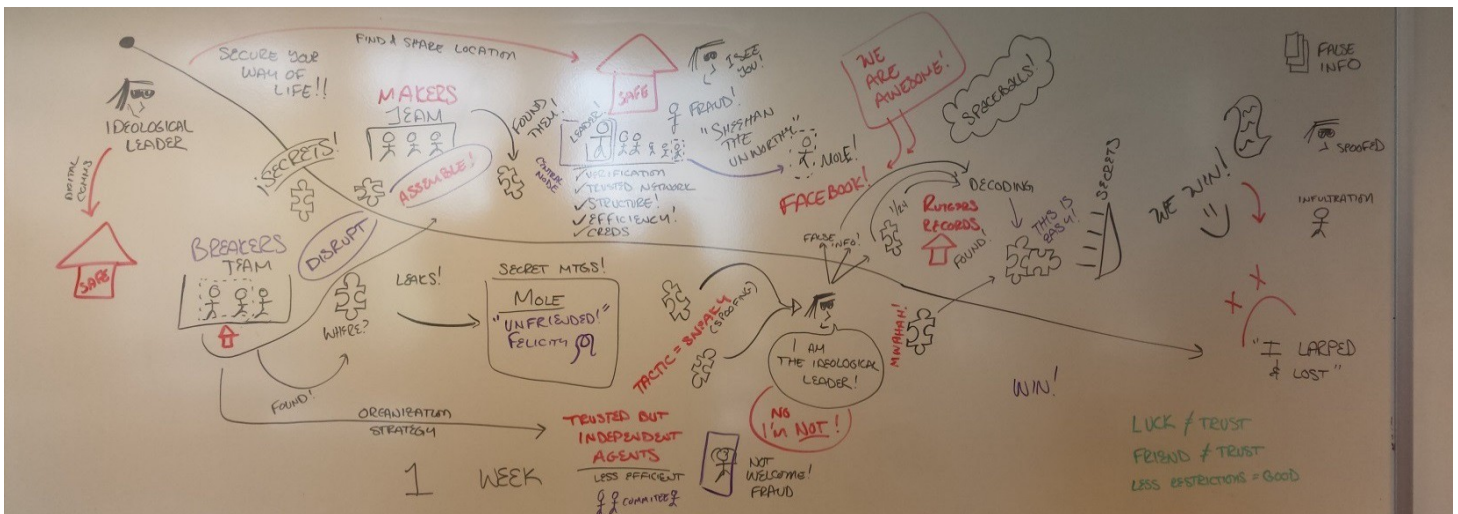
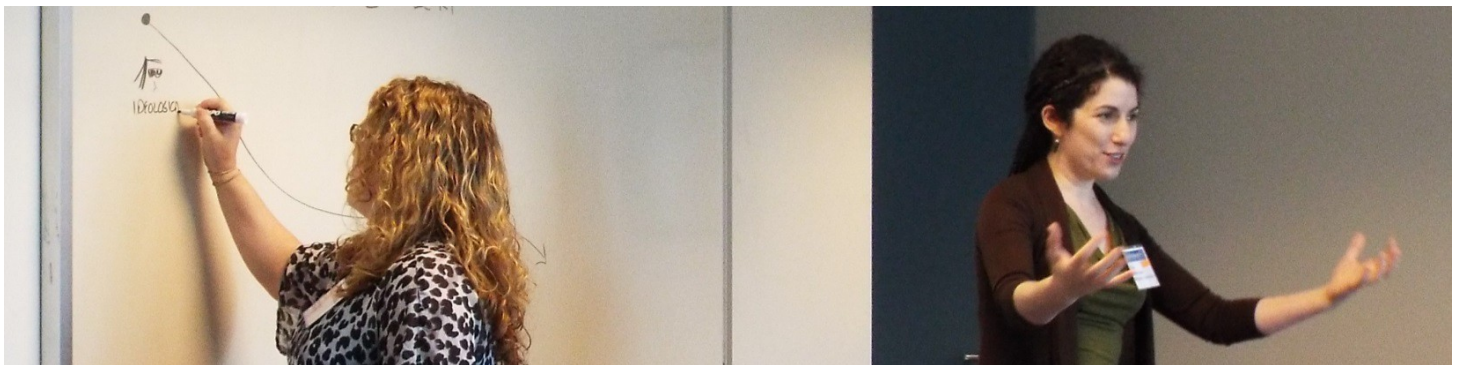


Figure 11: To inspire creative thinking of the Sandpit participants, Nina Fefferman and Emily Saulsgiver teamed to some storytelling and graphic facilitation during the lunch hour. Photo credit: James Wojtowicz.

One team - The Breakers - realized that to win, they didn't have to find all of the pieces of the puzzle; they just had to make sure the other team didn't find enough of the puzzle to solve the problem. True, but they had been told this at the beginning of the game. Their tactic changed from assembling puzzle pieces to disrupting the finding and assembling of the other team. They spoofed the identity of The Ideological Leader to provide misinformation to the other team on the location of puzzle pieces, managed to infiltrate the ranks of the other team (broke through the trust protocols established), and recreated clues and puzzle pieces themselves to mislead the other team.

The other team - The Makers - were highly organized, employed strict security protocols, with a natural leader taking on the coordination and communications activities of the team. They were effective, smart, and highly productive. However, they did not catch the mole who had infiltrated, nor did they catch the misinformation that slipped through. At the end of

the week, The Makers were confident they had achieved their mission and solved the puzzle. Instead, they found out they solved the wrong puzzle and had been deceived by someone in their own ranks.

The Breakers managed to mislead the Makers in three different ways: "identity" for their Mole, "identity" for their spoofed emails from The Ideological Leader, and the integrity of the puzzle pieces themselves.

RESEARCH AND DEVELOPMENT CONCEPT GENERATION

Following lunch and the report outs from the breakout groups, participants were invited to break into self-selected small groups to begin to develop research and development concepts to address the issues and challenges raised in discussions. Drafts of the concept templates were posted to the front of the room for others to review. Under each template an envelope collected comment forms, each of which is found in Figure 12.

CyDENTITY RESEARCH CONCEPT TEMPLATE	
A) Proposed Research Concept Name:	
B) Contributing Participants and Kibitzers:	C) Relevant CyDentity Theme(s) – Check one or more <input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input type="checkbox"/> Provenance for the "Internet of Things" <input type="checkbox"/> Metrics for Trust <input type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible.	E) Outline of Research Concept Proposed; What's New About it?
F) Which Disciplines are Necessary to Conduct the Research?	G) How Will You Evaluate Progress and Measure Effectiveness?
H) What research timeframe will be needed to address this Research Concept? <input type="checkbox"/> Short term (1-2 years) <input type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential "risks" associated with this approach?


CyDentity Sandpit 	
Name:	
<input type="checkbox"/> I Support this Concept – provide short explanation	
<input type="checkbox"/> I Can Contribute to this Concept – provide short explanation	
Other Comments:	

Figure 12: Concept Template and Feedback Form to be completed by CyDentityParticipants.



Figure 13: Small groups formed to develop research concepts. Photo credit: James Wojtowicz.

Each concept team was asked to address the following in their Concept Template:

- A) Proposed Research Concept Name
- B) Contributing Participants and Kibitzers
- C) Relevant CyDentity Theme(s) – Check One Or More
 - ☐ Identity Proofing in the Era of Social Media and Data Breaches
 - ☐ Provenance for the "Internet of Things"
 - ☐ Metrics for Trust

- ☐ Other (Please Describe Briefly)
- D) Brief Description of Problem Addressed by this Research Concept: Why is the problem difficult? Provide specific instances or concrete examples of the problem where possible.
- E) Outline of Research Concept Proposed; what is new about it?
- F) Which Disciplines are Necessary to Conduct the Research?
- G) How Will You Evaluate Progress and Measure Effectiveness?
- H) What Research Timeframe Will Be Needed To Address This Research Concept?
 - ☐ Short Term (1-2 Years)
 - ☐ Mid-Term (3 Years)
 - ☐ Long-Term (5 Years)
- I) What are the Potential "Risks" Associated with this Approach?

PROVOCATEUR PANEL 2: INSIGHTS FROM THE DAY



Figure 14: Wilson, Nash, and Glazer offer feedback on the draft CyDentity templates. *Photo credit: James Wojtowicz.*

In searching for clusters around similar topics, there were some around visualization and leveraging interactions in IT settings (analytics, management perspective), but do not limit this to IT. If you do link analysis, think about structures where it is standard. See what specialization is needed for each node.

There is an interesting question about bootstrapping new devices. How do we handle that? There is good research in the area of Limited Liability Persona but it needs more study to operationalize.

The impression is many of the proposals are non-technological. I would have guessed seeing more diving in and leveraging smart devices and wearable technology and being more "techie". One of contributions in the breakouts is looking at biology and ecology as alternative discipline approaches but some hard tech was absent. Additionally, we should stop wasting time defining things and accept some uncertainty to move forward. Perhaps analysis paralysis about the identity industry occurs when we begin discussions.

Behavioral evaluations are focused on what baseline activities look like (i.e. group, self). Behavioral evaluation when the individual is aware is essentially participatory surveillance but must come with privacy assurances. People may be willing to participate but there is a need to understand privacy ramifications.

Practically, the one thing is to understand privacy risks from social networking. There is a big problem out there about research of peoples mental models are of information, not a mental model of how info flows online. This is important for data service providers which powers the digital economy. You get an interesting discussion between those making money from data and privacy advocates. The Zuckerbergs collect participant data for a service system and people know it. I don't think they are knowledgeable and it's similar about the tobacco proposition - that adults knew risks. People may be exploited by ignorance. Out of the University of Pennsylvania, there is an argument that people give up data because people receive something of value in return. This is not true but they're fatigued and think they will lose information anyway. Mental models are lacking. To understand online risks and risky decisions people make, they need to understand those risks.

The PIV proposal to do a cost-benefit of the system is interesting. The proposer could think about PIV or smart cards more generally. There is privacy fear in smart cards. Other projects in similar area were torpedoed by privacy fear. Government smart cards are sim cards. The idea that the government is surveilling you is not different than other cards. Look at British of Columbia's health card. It's an EMV chip card and acts as issuer. They use off the shelf technology as smart card base. Customer engagement would be interesting to determine their concerns. Articles exist and may be of interest that may be a model for technologies people find unsettling and how do you tease it out and engage the public. If we do not include these types of things into projects, it may prove projects are unproductive.

Smart technology fails for all kinds of reasons. Hard problems exist in all the spaces we are looking at. The proposal involves sharing information. It is a hard problem but most want to receive information because it helps them. But it is hard to accept. When you get to sharing information, it becomes harder. That information is derived statistically and that is why there is confidence level on this stuff. Sharing information in your own organization is amazingly tough. How do you solve it? You create a 3rd institution and the problem still remains difficult. What triggers are we looking at regarding sharing of information in a controlled fashion? Branch sharing information is something to look at. We have bad tools to be able to have real sharing to take place.

What does it take to become trusted intermediary? What would it take to become world's top seller of a product? You do not need to be the best seller to be intermediary. Law and customs can create trust in a role but not specific implementation of a rule. Notary or escrow services are one example in the physical world. It appears though, that it would take law at this point to establish a trusted role type that multiple people can implement services and not specifically know the person behind it. Verisign is about building perception. The reason you don't jump start an identity provider is there are 2 problems: 1) You really have to invest a lot in brand and 2) if you start from scratch you run into coverage problem. This began to change about 3 years ago to the point where Facebook is no longer needed.

Think about what product the government can provide that would be attractive to all those customers. Almost all citizens are part of the homeland security enterprise as interactions between DHS and citizens occur. There is a need to apply pressure to gain access to secure elements of phones today and lubricate PKI.

CONCEPT REFINEMENT AND GROUP CANVASSING

The participants were provided additional time to continue to finalize their concept templates, while also reviewing what others were preparing and asking questions of the provocateurs and the government sponsors. Final drafts of the templates were posted to the front of the room for group canvassing and comments.



Figure 15: Canvassing of Participant Concepts. Photo credit: EmilySaulsgiver.

DAY 2 OPENING REMARKS AND CONCEPT PRESENTATIONS

The project team presented the findings at the end of Day 1. Each concept provided at the end of Day 1 was placed into at least one of six categories: the original IDAM Competency Areas, as well as an 'other' category. Concepts were

allowed to fall into up to two competency areas. A good number fell into the authentication and risk categories. The rest had on average three to four concept proposals.

As was witnessed at the end of Day 1 and the conversations that were happening, proposals became much more interesting once they were explained and not just put down on paper. Further, the templates required more description, especially in the area of research and development. Therefore, to help the concept teams think through each of their concepts more fully, each concept team gave a short summary of their concept. The concept author teams were asked to provide two minute summary presentations on their concept, and then five minutes for questions and comments from the group. The primary purpose of the concept summary presentation was to explain the end goal of each of the proposed concepts and allow for an exchange of interesting ideas amongst the rest of the participants.

Following the short presentations, concept teams were given the rest of time to finalize their original concept, combine concept ideas with other teams, or develop other concepts that came out of the group discussions. By the end of the day, final concepts were to be turned in, with a focus on impact and innovation.

CYDENTITY SANDPIT CONCEPTS

The following outlines the Concept Templates received by the end of the CyDentity Sandpit and how they align to the CyDentity Sandpit Theme Areas and the IDAM Capability Areas. For the full description on each concept, see Appendix C: CyDentity Sandpit Final Concept Templates.

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: 1:1 D Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access Control	User Experience	Other
1	Analytical Approaches for Understanding Risk, Benefits, and Trust Relationships			X	X		X				
2	Distributed Evaluation / Estimation of Trust	X	X	X			X				
3	Social Things: Self-Organizing Networks of Trust for the IoT		X				X				
4	Free Market Economy Based Attribution of Cyber Risk Exposures			X			X				
5	Catapulting Law Enforcement Investigations into the World of Cybercrime	X			X		X				
6	Bootstrapping Identity	X	X	X		X	X				
7	Limited Liability Persona: Bringing the Concept to Life	X		X			X				
8	Allowable Statements Using Metrics of Trust			X			X				

9	Identity Oracle: Proofing/Authentication against one's own behavior, biometric and other data	X				X					
10	Multi-Model Behavior Confidence Measurement for Identity Proofing	X		X		X	X				
11	Smartcard Technology to be used in Drivers Licenses: cost benefit assessment to society	X	X	X		X					
12	Transparency of Federation Hubs			X	X	X			X		
13	Identity Management in Support of Telecommunications Services Authorization for Emergency Communications	X	X			X			X		
14	Identity for Access to Critical Communications during Crisis				X	X			X		
15	Short Text Proactive Authentication	X	X			X					
16	Enabling Social Media Consumers to Understand Privacy Risks	X					X			X	
17	Transaction History of Trusted 3rd Party / Intermediate Operations		X	X				X		X	
18	A Visual Analytic Approach for Analysis and Response to NAT and IoT Attacks		X					X		X	
19	Digital Transformation Innovation Laboratory	X	X	X	X						X
20	Landscapes and Field Guides: Sense Making for Collaboration and Projects Research									X	X
21	Digital Torn Dollar	X		X	X			X			
22	Context, History, Power, Trust of Cyberspace	X	X		X						X

23	Intersecting Realms of Adaptive Provenance		X					X			
24	Combined with 15										
25	Blinded 3rd Party (Federation Hub)			X	X			X			X
26	Leveraging Federation Hubs for Non-Web		X					X			
27	Augmented Trusted 3rd Party with Security Notifications	X		X				X			
28	Personal Management in the Wild				X	X					
29	Global Survey of State to Citizen ID (eID) systems: a comparative eID open source research project			X	X						X
30	How does Nature do "Identity"? Applying Biomimicry to Key Concepts of Trust, Authentication, and Security				X						X
		14	12	15	11	9	10	7	3	4	6
		Theme 1: 1:1 D Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other

NEXT STEPS:

The CyDentity Sandpit was deemed to be successful based on participant feedback, found in Appendix D, and the reactions of the government sponsors at the event. Moving forward, CSD will need to maintain the momentum gained by the sandpit. Key functions of this momentum will include getting expressions of interest from internal and external customer perspectives in the CyDentity concepts so IDAM-E and CSD can start to prioritize and move quickly in the right direction. A community engagement strategy for identity, which must incorporate in-person meetings, will help CSD and IDAM-E organize and document identity activities, key events, points of contact, and impact to the homeland security enterprise.

APPENDIX A: CYDENTITY SANDPIT AGENDA



JUNE 29-JULY 1, 2015

Hosted by:

CCICADA Center of Excellence, Rutgers University, the State University of NJ - Busch Campus
7th Floor (Room 701), CoRE Building | 96 Frelinghuysen Road, Piscataway, NJ 08854-8018



Sponsored by:

U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Cyber Security Division (CSD)

WELCOME RECEPTION (JUNE 29):

5:30-7:30pm

Welcome Reception

The Old Bay Restaurant - New Jersey's premier New Orleans-style restaurant!
61-63 Church Street, New Brunswick, NJ 08901
Website: <http://www.oldbayrest.com/>

DAY 1 (JUNE 30): 8:00AM – 5:00PM

Topic	Discussion Details	Who	Location	Start
Registration & Coffee	Registration	ALL	Rm 701	8:00 AM
Welcome and Opening Remarks	<ul style="list-style-type: none"> - Welcome from CCICADA/Rutgers - Welcome from DHS S&T CSD - Background on DHS S&T CSD's interest and vision - Meeting objectives, attendees and format 	Fred Roberts, Rutgers University Doug Maughan, DHS S&T Joseph Kielman, DHS S&T Emily Saulsgiver, Meeting Facilitator	Rm 701	8:30 AM
Session A: Provocateur Panel	<ul style="list-style-type: none"> - What are the gaps in identity research? - What does this community need to focus on? 	Anil John (Moderator), DHS S&T Andrew Nash, Confyrm Ian Glazer, Salesforce Steve Wilson, Lockstep	Rm 701	9:00 AM
Session B: Review Theme Challenge Statements	<ul style="list-style-type: none"> - Are we missing anything in the Themes? - Overview of Breakout Group objectives - Introduce Concept Templates 	Emily Saulsgiver	Rm 701	10:00 AM
Networking Break		All	Rm 701	10:20 AM
Session C: Break-out into Concept Groups	<ul style="list-style-type: none"> - Discuss research challenges within Theme 1: Identity Proofing in the Era of Social Media and Data Breaches - Determine research domains required to address 	Kaliya, Leola Group (Moderator) Jonathan Bullinger, Rutgers University (Knowledge Agent)	Rm 701	10:40 AM
	<ul style="list-style-type: none"> - Discuss research challenges within Theme 2: Provenance for the "Internet of Things" - Determine research domains required to address 	Dave Thurman, Pacific Northwest National Laboratory (Moderator) Charles File, Rutgers University (Knowledge Agent)		



Command, Control, and
Interoperability Center for
Advanced Data Analysis
A Department of Homeland Security
Center of Excellence

	- Discuss research challenges within Theme 3: Metrics for Trust - Determine research domains required to address	Dennis Egan, Rutgers University (Moderator) Ryan Whytlaw, Rutgers University (Knowledge Agent)		
Lunch	Luncheon Presentation	Nina Fefferman, Rutgers University	Rm 401	12:00 PM
Session D: Group Lightning Summaries	- Short brief-out by Moderators on Breakout discussion high-points	Kaliya, Dave Thurman, and Dennis Egan	Rm 701	1:00 PM
Session E: Gallery Walk & Research Theme Development	- Self-organizing small groups - Draft templates on potential research efforts to address aspects of challenge statements	ALL	Rm 701	1:30 PM
Networking Break		ALL	Rm 701	2:30 PM
Session F: Provocateur Panel 2 – Insights from the Day	- Further Comments to the group based on breakout groups and concept discussions	Anil John (Moderator) Andrew Nash Ian Glazer Steve Wilson	Rm 701	2:45 PM
Session G: Concept Refinement & Posting	- Refine templates and add to the front wall	ALL	Rm 701	3:45 PM
Session H: Concept Canvassing / Adjourn	- Canvassing options: (A) support this concept, (B) Support and can provide additional expertise	ALL	Rm 701	4:30 PM
CyDentity Project Team Meeting	Closed Meeting	CyDentity Organizers	Rm 701	5:00 PM

6:30pm CyDentity Sandpit Dinner
Panico's
103 Church Street, New Brunswick, NJ 08901
Website: <http://www.panicosrestaurant.com/>

DAY 2 (JULY1): 8:00AM – 1:00PM

Topic	Discussion Details	Who	Location	Start
Registration, coffee, and networking	Registration	ALL	Rm 701	8:00 AM
Welcome and Opening Remarks	- Recap of Day 1 - Discussion of high-level findings of Concept Themes - Identify where others may contribute to these ideas	Anil John Joseph Kielman Emily Saulsgiver	Rm 701	8:30 AM
Session I: Concept Team Talks and Group Discussion	- Author teams give overview of concept (5 minutes each) - Group discussion	Concept Teams	Rm 701	9:00 AM
Working Lunch	Concept Template Refinement - Author teams update and build-out concepts based on group discussion	ALL	Rm 401	12:00 PM
CyDentity Sandpit Concludes	- Turn in final templates	Joseph Kielman, Anil John, Emily Saulsgiver	Rm 401	1:00 PM

APPENDIX B: PARTICIPANT SHORT BIOS

*Indicates Session Moderator

CYDENTITY PROJECT TEAM

Bullinger, Jonathan	Mr. Bullinger is currently a Doctoral Candidate and Graduate Assistant for CCICADA. Projects he has been involved with include Urban Commerce and Security Study (UCASS), Safety Act Phases I & II, and Stadium Security. A media studies scholar in the Department of Communication at Rutgers University, Jonathan's dissertation focuses on collective memory of war in the U.S.
Egan, Dennis*	Dr. Egan joined the Command Control Interoperability Center for Advanced Data Analysis (CCICADA) at Rutgers University as Research Professor in July, 2013. Earlier that year he retired from Applied Communications Sciences and its predecessor companies (Bell Laboratories, Bellcore, and Telcordia Technologies) after a 36-year career in research and research management focused on information and behavioral sciences and data analytics. Since arriving at CCICADA, Professor Egan has been involved in a great variety of research projects sponsored by the Department of Homeland Security. He co-authored a report on cybersecurity education for the DHS S&T Cyber Security Division (CSD). The report identified important ongoing cyber security educational efforts, and put forth recommendations for a cybersecurity education initiative for DHS. He also helps manage several ongoing cybersecurity research projects involving collaborations with other universities and government institutions. Professor Egan is currently technical lead for a project that is proposing security metrics for large sporting and entertainment venues. He was previously the technical lead for the EDGE Virtual Training and Transition project that evaluated a software system providing virtual training for teams of first responders. Egan received the A.B. degree from the College of the Holy Cross, and M.A. (Applied Mathematics) and Ph.D. (Experimental Psychology) from the University of Michigan. He was named Bellcore Fellow in 1992.
File, Charles	Charles File is a doctoral candidate in the School of Communication and Information at Rutgers University. He has a background in computer science and communications, and combines these interests by using computational techniques to study human behavior. His work in homeland security includes a three-year DHS Fellowship, a four-year association with the CCIADA research group that included work on projects such as stadium security and Coast Guard data integrity, and an internship at the Lawrence Livermore National Lab working on cyber-security.
John, Anil*	Anil John is a digital security coach. He helps technical leaders gain clarity and understanding on complex identity, information security and privacy practices, so they can enable secure, trustworthy digital services. He has been a civil servant, web developer, enterprise architect and professor. He has lead multi-disciplinary teams, developed and influenced government-wide identity and security policies, and managed the U.S. Government's Federal Identity, Credential and Access Management (FICAM) Trust Framework Solutions (TFS) Program, which enables government agencies to deliver citizen and business facing digital services in a secure, privacy respecting and interoperable manner while utilizing private sector identity services.
Kielman, Joseph	Within the U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T), Dr. Kielman is a Science Advisor for the Cyber Security Division, and also manages the Center of Excellence for Visualization and Data Analytics (CVADA) for the Office of University Programs. Prior to joining DHS S&T in 2003, he worked for 20 years at the FBI. There he served as Chief of the Advanced Technology Group for the Engineering Section, Chief of Research and Development in the Technical Services Division, and Chief Scientist and Chief Architect for the Information Resources Division. Dr. Kielman worked for the American Society for Testing and Materials, MCI Communications, and the Department of Health and Human Services prior to joining the FBI. Among other interagency assignments, he has chaired two subcommittees for the White House Office of Science and Technology Policy National Science and Technology Council, as well as serving on four Advisory Committees for the U.S. Department of Energy Pacific Northwest National Laboratory. Dr. Kielman has an undergraduate degree in Physics, graduate degrees in Biophysics, and did his postdoctoral work in Genetics. He was awarded the Presidential Rank of Meritorious Senior Professional in 2006.
Maughan, Douglas	Dr. Maughan is the Cyber Security Division Director in the Homeland Security Advanced Research Projects Agency (HSARPA) within the Science and Technology (S&T) Directorate of the Department of Homeland Security (DHS). Dr. Maughan has been at DHS since October 2003 and is directing and managing the Cyber Security Research and Development activities and staff at DHS S&T. His research interests and related programs are in the areas of networking and information assurance. Prior to his appointment at DHS, Dr. Maughan was a Program Manager at the Defense Advanced Research Projects Agency (DARPA) in Arlington, Virginia. Prior to his appointment at DARPA, Dr. Maughan worked for the National Security Agency (NSA) as a senior computer scientist and led several research teams performing network security research. Dr. Maughan received Bachelor's Degrees in Computer Science and Applied Statistics from Utah State University, a Master's degree in Computer Science from Johns Hopkins University, and a PhD in Computer Science from the University of Maryland, Baltimore County (UMBC).

Roberts, Fred Dr. Roberts is a Distinguished Professor of Mathematics at Rutgers University and Director of the Command, Control, and Interoperability Center for Advanced Data Analysis (CCICADA), a University Center of Excellence of DHS. He is Emeritus Director of DIMACS, the Center for Discrete Mathematics and Theoretical Computer Science, one of the original National Science Foundation Science and Technology Centers, which he directed for 16 years. Roberts is a member of the Board on Mathematical Sciences and Applications, a former member of National Science Foundation advisory committees on International Research and Education, Mathematical and Physical Sciences, and Environmental Research and Education, is on the Steering Committee for the World-Wide Program Mathematics of Planet Earth, on the Scientific Advisory Committee to the Institute for Applied Systems Analysis (IIASA), co-chairs the NJ Universities Homeland Security Research Consortium, has served on the Secretary's epidemiology modeling group at the Department of Health and Human Services, and serves on the NJ Governor's Health Emergency Preparedness Advisory Council and the NJ Domestic Security Preparedness Task Force Planning Group. Roberts is the author of four books, editor of 21 additional books, and author of over 180 scientific articles and deals with a wide variety of topics, including mathematical models addressing problems of homeland security, energy modeling, decision making, communication networks, mathematical psychology, measurement, epidemiology, computational biology, sustainability, and precollege education. Among Dr. Roberts' current homeland security research interests are stadium security, resource allocation (e.g., for Coast Guard boats and aircraft), container inspection at ports, sensor management for nuclear detection, early warning of disease outbreaks and bioterrorist events, border security, behavioral responses to natural and human-caused disasters, the connection between security and economic activity, and the homeland security aspects of global environmental change. Professor Roberts has received a University Research Initiative Award from the Air Force Office of Scientific Research, the Commemorative Medal of the Union of Czech Mathematicians and Physicists, and the Distinguished Service Award of the Association of Computing Machinery Special Interest Group on Algorithms and Computation Theory, and he is a Fellow of the American Mathematical Society. He also received the NSF Science and Technology Centers Pioneer Award in a ceremony at NSF and received an honorary doctorate from the University of Paris-Dauphine.

Saulsgiver, Emily Ms. Saulsgiver is a Government Consultant with TechOp Solutions International, Inc. She has worked with DHS S&T since 2007 providing program management, facilitation, and technical writing support in the areas of cybersecurity, visualization and data analytics, first responder technologies, and DHS operational component mission and engagement strategy. Before DHS S&T, Ms. Saulsgiver supported research initiatives at DARPA in the area of interoperable communications. Outside of TechOp, Ms. Saulsgiver volunteers with DC Stop Modern Slavery as Director for Community and Organizational Outreach. She begins her graduate studies in International Relations and Public Policy this summer at the University of New South Wales in Sydney, Australia.

Whytlaw, Ryan Ryan Whytlaw is a Senior Research Specialist with CCICADA, a DHS Center of Excellence at Rutgers, The State University of New Jersey. Mr. Whytlaw also provides research support to the Alan M. Voorhees Transportation Center at the Bloustein School of Planning and Public Policy. Mr. Whytlaw has more than 10 years of experience in the field's emergency management and public safety. He supports a variety of research and planning projects involving a range of policy topics such as emergency management and operations, hazards risk assessment, security, mitigation, climate change adaptation and disaster resiliency. His experience includes supporting research projects involving all-hazards emergency management and evacuation planning, entertainment venue and stadium security, transportation systems disaster resiliency, health impact assessments, as well as crafting cost-benefit policies and processes in these policy areas.

Prior to joining Rutgers, Mr. Whytlaw was employed with the Metropolitan Washington Council of Governments (MWCOC) as a public safety planner under both the Council of Governments and its associate organization the National Capital Region (NCR) Transportation Planning Board. His work included the coordination of evacuation planning efforts between federal, state, county, and local agency representatives in the NCR under the Emergency Support Function (ESF) 1 – Transportation Committee as committee lead for MWCOC. Mr. Whytlaw further acted as committee lead to the NCR's Fire Chiefs under ESF-4 along with many other efforts focusing on emergency management and public safety issues. Additionally, Mr. Whytlaw spent time at CSR, Incorporated, where he supported multiple US DHS projects including the administering of the Commercial Equipment Direct Assistance Program (CEDAP) requiring review of emergency procedures and protocols. He obtained his master of public policy from George Mason University and completed his undergraduate studies at Albright College.

PROVOCATEURS AND LUNCHEON SPEAKER

Fefferman, Nina Dr. Fefferman is interested in mathematical, biological, and social questions stemming from complex systems (systems in which the rules governing the behavior of each component are relatively simple, but the components react to each other to create highly organized and incredibly complex behaviors). Her work ranges from basic scientific questions (such as the influence of infectious disease on the evolution of social behaviors in animals, the impact of ongoing dynamics to transmission processes on shifting networks, etc.) to practical applications (such as designing detection algorithms for cyberattacks, determining how best to maintain critical societal infrastructure in the face of pandemic disease, and exploring the impact of social leadership in whether or not people default on their home mortgages, etc.). Two important and related cross-cutting themes in her work are (a) how individuals can use locally available knowledge to achieve globally efficient outcomes, and (b) how groups of individuals collaborate to construct understanding. Dr. Fefferman received her AB in Mathematics from Princeton University, her MS in Mathematics from Rutgers University, and PhD in Biology from Tufts University.

Glazer, Ian Ian Glazer is the Senior Director for Identity, at Salesforce. His responsibilities include product strategy, identity standards development, field enablement, analyst relations, and mindshare generation. Mr. Glazer is also involved with major customer initiatives, briefs C-level executives, and coordinates industry-wide identity efforts. Mr. Glazer was a research vice president and agenda manager on the Identity and Privacy Strategies team at Gartner, where he oversaw the entire team's research. He arrived at Gartner by way of Gartner's acquisition of the Burton Group. He led the team's coverage for authorization and privacy; topics

within these two main areas included externalized authorization management, XACML, federated authorization, privacy by design, and privacy programs. Other topics he researched included user provisioning, identity and access governance, access certification, role management, identity data quality, and national identity programs. Mr. Glazer's other work experience includes program management at a financial controls and governance, risk and compliance startup, director of identity strategy at a network-based admissions control company, and product management at IBM.

Mr. Glazer is the current Vice-Chair of the Management Council and member of the Board of Directors for the Identity Ecosystem Steering Group (IDESG) – the private-sector lead body described in the US National Strategy for Trusted Identities in Cyberspace. He is also the Editor for the Kantara Initiative Identity Relationship Management Working Group. During his decade plus time in the identity industry he has co-authored a patent on federated user provisioning, co-authored the Service Provisioning Markup Language (SPML) Version 2 specification, contributed to the System for Cross Domain Identity Management (SCIM) Version 2 specification, and is an noted blogger, speaker, and photographer of his socks. Mr. Glazer graduated from the University of Pennsylvania cum laude with a Bachelors of Applied Science in Computer Science. He studied artificial intelligence at the University of Edinburgh. He currently resides in Washington DC.

Nash, Andrew Andrew Nash is the Chief Executive Officer at Conform. Prior to that, he was the Director of Identity Services at Google and Senior Director of Identity Service at PayPal. He has developed consumer identity vetting and verified information systems as CTO for Trulioo, and as CTO at Sonoma Systems and Reactivity built XML and Web Services Gateways. As Director of Technologies at RSA Security, he worked on a wide range of identity and security systems. Andrew has been a board member at the Open ID Foundation, Open Identity eXchange and the Information Card Foundation, and in 2006 was recognized by InfoWorld as one of the "Top 25 Most Influential CTO's of 2006."

Wilson, Steve Steve Wilson is Managing Director of Sydney-based identity and privacy advisory firm Lockstep Consulting, and a conjoint Vice President and Principal Analyst at San Francisco-based Constellation Research.

Steve has worked in digital identity and data privacy for 20 years, holding R&D leadership and Principal Consultant roles with Security Domain (later Baltimore Technologies), KPMG, PwC and SecureNet. In 2004, Steve founded Lockstep Consulting, and in 2014 he joined Constellation Research. Steve's undergraduate training was in physics and electrical engineering; prior to entering the IDAM industry he worked in implantable medical device in Australia and the U.S.

He is a passionate security innovator, and is responsible for several important innovations in PKI, privacy, and the "ecology" of digital identity. He has been awarded nine patents for digital identity and Privacy Enhancing Technologies.

PARTICIPANTS

Best, Daniel Daniel M. Best is a Cyber Security Researcher at Pacific Northwest National Laboratory. His research interests include visual analytics, cyber security, algorithm development, and applied graph theory. Best works on projects in support of government and lab directed research to enable innovative solutions. He has received PNNL's Key Contributor award for his work on visual analytic environments and has been awarded a patent on analyst investigation provenance.

Brennan, Joni Joni Brennan is the Executive Director of Kantara Initiative, focusing on Identity and Privacy Technology development to connect business, consumers, governments, citizens, and users to trustworthy on-line environments. Joni maintains guiding principles of openness and transparency to leverage 15 years proven experience in Identity Management innovation. She works to drive and formalize diplomatic and strategic partnerships between organizations. She participates in international government and industry organizations including: OECD ITAC, ISOC, IEEE-SA, OASIS SSTC, ISO SC27 WG5, and ITU-T. She has provided testimony regarding Trusted Identity and Access Management systems for the US ONC HITSP. Under her stewardship Kantara Initiative has delivered a verification program for the GSA FICAM and has developed open standards including the Identity Assurance Framework and User-Managed Access. She is a graduate with honors of Rutgers Douglass & the School of Communications Information and Library Sciences, with a Bachelors of Arts in Information Technology and Informatics.

Cooper, James Jim serves as the General Manager for Cyber Security Operations in the Chief Security Office of the Port Authority of New York and New Jersey. His responsibilities include the development of the organizations approach to cyber security operations to include the creation of a cybersecurity operations center and the coordination of related investigations. Prior to joining the cyber group, Mr. Cooper provided technical services to the Port Authority Police Criminal Investigations Bureau and the regional Joint Terrorism Task Force. In this role, Mr. Cooper provided a variety of technical services to include technical surveillance, video recovery/ enhancement and pattern analysis to support targeted law enforcement activities. Jim has more than 20 years of experience in incident management and physical security.

Cowell, Andrew Andrew Cowell is a senior research scientist and technical group manager at the Pacific Northwest National Laboratory. He leads a team of 50 researchers and engineering in the Visual Analytics group all focused on discovering, developing, and deploying innovative visual analytics technologies that enable timely and profound insights from complex data. His personal research interests focus on social media analytics, especially in regards to the exploitation of these sources and other open sources in aid of the DOE mission space. The majority of his work at PNNL has focused on aiding government analysts in interacting with massive data. His doctoral work, funded by Eastman Kodak, looked at methods to increase the perceived trust and credibility assigned to anthropomorphic computer characters. Prior to joining the lab in 2002, Andrew worked for British Telecom Research Labs and Eastman Kodak Research Labs. He holds a Computer Science B.Sc. First Class with a concentration in HCI (Univ. Of Bradford, UK), an M.Sc. in Cognitive Science (Univ. Of Manchester, UK) and a Ph.D. from the Univ. of Central Florida with a focus on Intelligent Interface Agents.

Diener, Debra Debra N. Diener served in senior managerial, legal, policy and legislative positions in all three branches of the Federal Government. She was one of the first co-chairs of the Identity Management Subcommittee of the CIO Council's Privacy Committee. She did so while serving as the Deputy Director for Privacy Policy at the IRS and subsequently as the Senior Advisor and Deputy Director for Privacy Policy at the Department of Homeland Security. She is now an independent consultant providing strategic guidance to industry and non-profit organizations on a wide-array of privacy and identity management issues. Ms. Diener is a

frequently requested speaker. She received her B.A. *cum laude* from Syracuse University, her M.A. from the University of Pennsylvania and her J.D. *with honors* from the George Washington University. She is also a Certified Information Privacy Professional with a Government specialization.

- Gebel, Gerry** Gerry Gebel is President, Axiomatics Americas where he is responsible for sales, customer support, marketing and business development for the Americas region. Prior to Axiomatics, he was VP and service director for Burton Group's identity management practice, where he also published reports on authorization, federation, access governance, user provisioning and other IAM topics. Gerry has also been active in advancing the use of identity standards, having led interoperability projects for authorization, federation and user centric specifications. In addition, Gebel has nearly 15 years' experience in the financial services industry including architecture development, engineering, integration, and support of Internet, distributed, and mainframe systems.
- Kaliya*
a.k.a. Identity
Woman** Kaliya "Identity Woman" is an independent advocate for the rights and dignity of our digital selves. In 2005 she co-founded the Internet Identity Workshop (with Doc Searls and Phil Windley), five years later she founded the Personal Data Ecosystem Consortium to catalyze a network of companies working to give individuals the tools to collect, manage and gain value from their own personal data generated actively and passively as they interact with all kinds of digital systems. Kaliya was actively recruited to participate in the NSTIC process and was elected three times to the Management Council of the Identity Ecosystem Steering Group before resigning in February 2015. In 2012 Hamlin was named a Young Global Leader in 2012 by the World Economic Forum (WEF).
- Ho, Fenton** Fenton Ho is the Director of Cyber Authentication and Identity Management at the Treasury Board Secretariat (TBS) of Canada where he oversees the development of identity management policy for the government of Canada. He is also the Technical Lead for Canada's Digital Interchange Taskforce where he is responsible for all technology related aspects of this Pan-Canadian initiative to transform how identity information is exchanged. Prior to joining TBS, he established and led the strategic intelligence program at FINTRAC, Canada's financial intelligence agency. Fenton holds a Ph.D in Systems Design Engineering from the University of Waterloo where his research focus was on artificial intelligence and machine learning. He began his career in fraud and risk management in the banking sector.
- Jain, Ashish** Ashish Jain is VP of Data Analytics and Business Intelligence at iconectiv, a wholly owned subsidiary of Ericsson. iconectiv is a leading provider of Interconnection Solutions for the Communication Services industry and is an authoritative source of several critical reference data sources related to network infrastructure and call and messages routing. Ashish has lead R&D and technology transfer initiatives in the areas of next generation carrier grade voice and data services platforms, repositories and clearinghouses for secure exchange of private information, and infrastructure for creating secure online marketplaces. For the CyDentity Sandpit, Ashish is most interested in identification of unconventional authoritative reference data sources for establishing provenance of data/objects.
- Kantor, Paul** Paul Kantor, Ph.D. is Distinguished Professor of Information Science at Rutgers (Emeritus, as of July 1, 2015) and a founding editor of the journal Information Retrieval. He serves as Research Director of the CCICADA Center for Advanced Data Analysis, and has worked on information retrieval systems design and evaluation since 1972. He is a Fellow of the American Association for the Advancement of Science, a Senior Life Member of the IEEE and a member of the American Statistical Association, ASIST and the ACM. He is co-Editor of the Springer Recommender Systems Handbook first edition. His research has been supported by NSF, ARDA, DARPA, DHS, ONR, and other organizations. At Rutgers he is also a member of DIMACS Center for Discrete Mathematics and Computer Sciences; and on the graduate faculties of Computer Science and Operations Research. The author of over 200 papers and technical reports, he is particularly interested in the problems of estimating and utilizing indicators of confidence, about both data and metadata. These problems become ever more important as humans and algorithms work, in ever closer coupling, to make critical decisions.
- Koven, Jay** Jay Koven is a third year PhD Candidate in Computer Science Engineering at NYU Polytechnic School of Engineering working with professors Nasir Memon and Enrico Bertini. His current research focuses on Data Forensics and Visual Data Analytics on large email datasets. His current research is in collaboration with the United States Secret Service Cyber Crime Unit in New York City and the New York County District Attorney's Office. Before starting work on his Doctorate he worked at Digital Equipment Corporation and ATEX publishing systems on various desktop publishing and computer human interaction projects. He BS is from Worcester Polytechnic Institute and his MS is from Iona College.
- Lindqvist, Janne** Janne Lindqvist is an assistant professor of electrical and computer engineering and a member of WINLAB at Rutgers University, where he directs the Rutgers Human-Computer Interaction group. From 2011-2013, Janne was an assistant research professor of ECE at Rutgers. Prior to Rutgers, Janne was a post-doc with the Human-Computer Interaction Institute at Carnegie Mellon University's School of Computer Science. Janne received his M.Sc. degree in 2005, and D.Sc. degree in 2009, both in Computer Science and Engineering from Helsinki University of Technology, Finland. He works at the intersection of human-computer interaction, mobile computing and security engineering. Before joining academia, Janne co-founded a wireless networks company, Radionet, which was represented in 24 countries before being sold to Florida-based Airspan Networks in 2005. His work has been featured several times in IEEE Spectrum, MIT Technology Review, Scientific American, Yahoo! News and recently also in Computerworld, Der Spiegel, London Times, International Business Times, Fortune, CBS Radio News, NPR, WHYY Radio, and over 300 other online venues and print media around the world. During his first year at Rutgers, Janne was awarded three NSF grants totaling nearly \$1.3 million and a MobiCom best paper award. Janne recently received UbiComp best paper nominee award (UbiComp 2014, 4% of papers). Janne is a professional member of AAAS, ACM and IEEE.
- Maciejewski, Ross** Ross Maciejewski has been an Assistant Professor of Computer Science at Arizona State University since 2011. Prior to joining Arizona State University Dr. Maciejewski completed his PhD at Purdue University in Computer Engineering. He then served as a visiting faculty member at Purdue as a member of the Department of Homeland Security's Center of Excellence focusing on visual analytics (VACCINE). His work at Purdue's VACCINE Center was honored by the United States Coast Guard with a Meritorious Team Commendation as part of his work on the Port Resilience for Operational Tactical Enforcement to Combat Terrorism (PROTECT) Team. Dr. Maciejewski's primary research interests are in the areas of geographical visualization and visual analytics focusing on public health, social media, criminal incident reports and dietary analysis. He has served on the organizing committee for the IEEE Conference on Visual Analytics Science and Technology (2012-2013, 2014) and for the EuroVis Conference (2014,

2016), is an NSF CAREER award winner (2014), and has been involved in award winning submissions to the IEEE Visual Analytics Contest (2010 and 2013). For more information on his current work visit vader.lab.asu.edu.

Manz, David

David Manz is currently a Staff Cyber Security Scientist in the National Security Directorate at the Pacific Northwest National Laboratory. He holds a B.S. in Computer and Information Science from the Robert D. Clark Honors College at the University of Oregon and a Ph.D. in computer science from the University of Idaho. David's work at PNNL includes enterprise resilience and cyber security, secure control system communication, and critical infrastructure security. Prior to his work at PNNL, David spent five years as a researcher on Group Key Management Protocols for the Center for Secure and Dependable Systems at the University of Idaho (U of I). David also has considerable experience teaching undergraduate and graduate computer science courses at U of I, and as an adjunct faculty at WSU. David has co-authored numerous papers and presentations on cyber security, control system security, and cryptographic keymanagement.

Martinez, Gabriel

Gabriel Martinez works in the Architecture and Advanced Technology team at the Office of Emergency Communications at DHS. Mr. Martinez currently supports OEC in the implementation of the National Emergency Communications Plan (NECP), Priority telecommunications Services evolution for National Security and Emergency Preparedness Communications (NS/EP), and Identity Credentialing and Access Management (ICAM) developments that affect the NECP Ecosystem. Prior to joining DHS, Mr. Martinez worked for the Department of Defense, National Communications System in the area of NS/EP. Mr. Martinez holds a B.S. in Electrical Engineering from University of Maryland at College Park and a M.S. in Electrical and Computer Engineering from John Hopkins University Applied Physics Lab.

Nolan, David

Mr. Nolan is an electronics engineer in the DHS Office of Emergency Communications working in the area of National Security and Emergency Preparedness communications. Prior to joining DHS in 2008, Mr. Nolan worked in the Defense Department designing Internet Protocol based communication systems. He was involved in deploying communications over satellite for first responders during Hurricane Katrina. His background includes several large network projects such as DOD Joint IP Modem at DISA and Common User Installation Transport Network (CUITN) at US Army CEECOM, as well as a previous assignment with DHS working on priority communications, investigating NGN technologies such as wireless and Internet Protocol based systems for NS/EP.

Pandey, Anshul Vikram

Anshul Vikram Pandey is a Ph.D. candidate in the computer science department at New York University - Polytechnic School of Engineering. His research focuses on information visualization and its role in decision making, and has published works at premier conferences, such as CHI and InfoVis. He received his B.E. (Hons., 2012) in electrical and electronics engineering from BITS Pilani, India and has previously worked in the field of human computer interaction, intelligent systems and wearable technologies.

Pottenger, Bill

Dr. Pottenger is CEO and founder of Intuidex, a manufacturer of solutions in the visual and data analytics space. Bill is also Director of Transition for CCICADA. He is also an Associate Research Professor at Rutgers University at DIMACS and RUTCOR in the Computer Science area. Bill is active in research and development of data analytics technology, and has received over \$6M in competitive research funding from the NSF, DHS, NIJ, ARL, industry, etc. as principal investigator, and as a co-investigator over \$30M, has over 40 peer-reviewed publications, has served as editor and chair of several proceedings/symposia and made over 50 professional presentations/seminars. Bill is a member of ACM, IEEE, SIAM and has served as a program committee member/referee for numerous professional venues, journals, etc. Among other awards he is the recipient of the PC. Rossin Endowed Assistant Professorship and a United States Air Force Certificate of Appreciation. Prior to coming to Rutgers, Bill completed his Ph.D. in Computer Science at the University of Illinois at Urbana-Champaign and worked as a Research Scientist at the National Center for Supercomputing Applications and at Lehigh University. Bill's research interests include the fields of statistical relational learning and information extraction as applied in Higher Order Learning, a framework he developed for both supervised and unsupervised learning based on higher-order relations. He is active in research in visual and data analytics and parallel and distributed computing as well. His company, Intuidex, Inc., creates leading-edge data analytics technology for use both at home and in business. Application domains of Intuidex technology include law enforcement, fortune 500 business, defense and counterterrorism.

Queralt, Michael

Michael Queralt, co-founder and president of Queralt Inc., is responsible for leading the efforts around the commercialization and operations of the cyber-security solutions, that have been developed under the sponsorship of the U.S. Department of Homeland Security – Cyber security Directorate. As its Principal Investigator, he has lead the research and development effort for Queralt's cyber physical decisioning platform and many of the attribute based access solutions. Queralt is currently working with the Identity Management test bed residing at John Hopkins University, Advanced Physics Lab and the Open Geospatial Consortium operated by George Mason University. He has extensive executive management experience with leading technology organizations and is and advisor to multiple start-ups focused around the use of the Internet of things for security, healthcare and industrial applications.

Rajagopalan, Raj

Dr. S. Raj Rajagopalan is a Senior Principal Research Scientist at Honeywell Automation and Control Systems (ACS) Research, where he leads a team of researchers tasked with creating appropriate security and privacy solutions for Honeywell's vast portfolio of control systems. Raj works closely with the various business units in ACS, especially the businesses that provide solutions for buildings control and management. Primary among his interests are challenges in the intersection of security, safety, and usability, especially because the typical usage of Honeywell products tends to be in safety-critical environments involving non-expert users. He is also working currently with the Security Operations Center organization in Honeywell to bring techniques from Anthropology to bear on human issues that challenge cyber security. Prior to joining Honeywell, Dr Rajagopalan worked with HP Labs Security Research Group where he worked on forensics and threat detection.

Roth, Dan

Dan Roth is a Professor in the Department of Computer Science and the Beckman Institute at the University of Illinois at Urbana-Champaign and a University of Illinois Scholar. He is the director of the DHS funded Center for Multimodal Information Access & Synthesis (MIAS) and has faculty positions also at the Statistics, Linguistics and ECE Departments and at the graduate School of Library and Information Science.

Roth is a Fellow of the American Association for the Advancement of Science (AAAS), the Association of Computing Machinery (ACM), the Association for the Advancement of Artificial Intelligence (AAAI), and the Association of Computational Linguistics (ACL), for his contributions to Machine Learning and to Natural Language Processing. He has published broadly in machine learning, natural language processing, knowledge representation and reasoning and learning theory, and has developed advanced

machine learning based tools for natural language applications that are being used widely by the research community. Prof. Roth has given keynote talks in major conferences, including AAAI, The Conference of the American Association for Artificial Intelligence; EMNLP, The Conference on Empirical Methods in Natural Language Processing, ECML & PKDD, the European Conference on Machine Learning and the Principles and Practice of Knowledge Discovery in Databases, and EACL, the European Conference of Computational Linguistics. He has also presented several tutorials in universities and conferences including at ACL and the European ACL and has won several teaching and best paper awards.

Roth is the Editor-in-Chief of the Journal of Artificial Intelligence Research (JAIR) and has served on the editorial board of several of the major journals in his research areas. He was the program chair of AAAI'11, ACL'03 and CoNLL'02 and serves regularly as an area chair and senior program committee member in the major conferences in his research areas. He has co-founded several start-ups in the Text Analytics area, and is consulting multiple small and large corporations on Text Analytics and Information Trustworthiness. Prof. Roth received his B.A Summa cum laude in Mathematics from the Technion, Israel and his Ph.D in Computer Science from Harvard University in 1995.

Sharkey, Tom

Thomas Sharkey is an Associate Professor in the Department of Industrial and Systems Engineering at Rensselaer Polytechnic Institute. His main research interests are in creating new optimization models and algorithms for infrastructure and supply chain resilience. In particular, his research has examined real-time algorithms to determine near-optimal restoration plans for disrupted infrastructure and supply chain networks and examined computational approaches to determine the value of information in restoration efforts. He is currently interested in how cyber-attacks can impact infrastructures and supply chains and also how to recover these systems from such an attack.

Simonsen, David

David Simonsen, head of Trust and Identity services at the Danish e-Infrastructure Cooperation (DeIC) is also manager of the Danish federation WAYF - Where Are You From. DS holds a master of IT from the IT University of Copenhagen and a bachelors degree in molecular biology from Copenhagen University, CISSP and ISO27001 L.I. certifications. DS has over the last decade been part of the global community for research and educational networks and is often presenting at conferences. DS was one of the founding fathers of the international wifi roaming service, 'eduroam' (now available in 74 countries) as well as the Nordic inter-federation effort Kalmar2.org. DS is member of an international group of governments focusing on citizen facing services, federated identity, LoA, user engagement, privacy etc.

Thurman, Dave*

Dave Thurman is Director, National Security Computing Programs at Pacific Northwest National Laboratory. In this role, he is responsible for working with government sponsors to define and initiate new research activities in the areas of data visualization and analysis, decision support, and cybersecurity across a range of national security mission challenges. He also oversees PNNL's Seattle Research Center with a focus on building partnerships with research institutions and technology companies in the greater Seattle area. Mr. Thurman has led numerous research programs to develop new analytic methods and capabilities for a range of federal organizations. He has previously conducted research on advanced knowledge representation techniques to support intelligence analysis, led efforts to define information integration architectures for the U.S. Department of Homeland Security, architected integrated modeling systems for natural resource management, studied information analysis methods at the International Atomic Energy Agency, and developed integrated analysis systems for a variety of government clients. Internally at PNNL, he has served in leadership roles for research initiatives on data-intensive computing, threat anticipation, and signature discovery. Mr. Thurman holds undergraduate degrees in Mathematics and Computer Science from the University of Oregon, and a Masters in Human-Machine Systems Engineering from Georgia Institute of Technology.

Windley, Phil

Phil Windley is an Enterprise Architect in the Office of the CIO at Brigham Young University. Previously he was the Founder and Chief Technology Officer of Kynetx, the company behind the open-source connected-car product, Fuse. He is the co-founder and organizer of the Internet Identity Workshop. He is also an Adjunct Professor of Computer Science at Brigham Young University where he teaches courses on reputation, digital identity, large-scale system design, and programming languages. Phil writes the popular Technometria blog and is a frequent contributor to various technical publications. He is also the author of the books The Live Web published by Course Technology in 2011 and Digital Identity published by O'Reilly Media in 2005. Phil spent two years as the Chief Information Officer (CIO) for the State of Utah in 2001-2002, serving on Governor Mike Leavitt's Cabinet and as a member of his Senior Staff. Before entering public service, Phil was Vice President for Product Development and Operations at Excite@Home. He was the Founder and Chief Technology Officer (CTO) of iMALL, Inc. an early creator of electronic commerce tools. Phil serves on the Boards of Directors and Advisory Boards for several high-tech companies. Phil received his Ph.D. in Computer Science from Univ. of California, Davis in 1990.

Wright, Rebecca

Rebecca Wright is a professor in the Computer Science Department and Director of DIMACS at Rutgers. Earlier, she was a professor in the Computer Science Department at Stevens Institute of Technology and a researcher in the Secure Systems Research Department at AT&T Labs and AT&T Bell Labs. Her research spans the area of information security, including cryptography, privacy, foundations of computer security, and fault-tolerant distributed computing, as well as foundations of networking. Dr. Wright serves as an editor of the International Journal of Information and Computer Security and of the Transactions on Data Privacy. She is a member of the board of the Computer Research Association's Committee on the Status of Women in Computing Research (CRA-W), and was a member of the board of directors of the International Association for Cryptologic Research from 2001 to 2005. She was Program Chair of Financial Cryptography 2003 and the 2006 ACM Conference on Computer and Communications Security (CCS) and General Chair of Crypto 2002, and has also served on numerous program committees. She received a Ph.D. in Computer Science from Yale University, a B.A. from Columbia University, and an honorary M.E. from Stevens Institute of Technology.

Wullert, John

John Wullert, PhD has had a varied career at Bellcore/Telcordia/Applied Communication Sciences. His initial work was in the area of flat panel display technologies and applications. Based on this and related work in the area of display technologies, John co-authored a book, Electronic Information Display Technologies. Subsequently, John investigated various aspects of optical signal processing, implementing an optical neural computer capable of learning the English alphabet and designing and implementing control electronics for shaping femto-second laser light pulses. Later, John worked with several opto-electronic technologies, including surface-emitting semiconductor lasers, and semiconductor and optical storage technologies. John also conducted experiments in educational applications of telecommunications technologies, devising techniques to allow museums to offer electronic field trips. Most recently as the Director of ACS's Next Generation Network and Data Services Research Group, John

has been involved with working with both next generation telecommunications services and big data analytics. In regard to telecommunications services, he is examining methods to ensure robustness and security of both the network infrastructure and the user data/equipment, particularly focusing on evolving government priority communication services to next generation networks. In data analytics, he is devising and implementing techniques for performing information extraction and classification of large corpora of text documents.

APPENDIX C: CYDENTITY SANDPIT FINAL CONCEPT TEMPLATES

Each concept template self-identified with one of the CyDentity Sandpit Themes or explained what else they were addressing. Following their completion, the templates were also identified to be in 1 to 2 IDAM capability areas. The final templates, their themes, and capability areas are captured below.

TEMPLATE 1: ANALYTICAL APPROACHES FOR UNDERSTANDING RISK, BENEFITS, AND TRUST RELATIONSHIPS

Authors: Sharkey, Pandley, Wullert, Martinez

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Proofing ID	Theme 1: Provenance	Theme 2: Metrics of Trust	Theme 3: Other	Authentication	Risk	Application Security	Access	User Experience	Other
1	Analytical Approaches for Understanding Risk, Benefits, and Trust Relationships			X	X		X				

CYDENTITY RESEARCH CONCEPT TEMPLATE	
A) Proposed Research Concept Name: Analytical Approaches for Understanding Risk, Benefits, and Trust Relationships	
B) Contributing Participants and Kibitzers: Thomas Sharkey, RPI Anshul Vikram Pandey, NYU Graduate Student John Wullert, Leidos (support to DHS NPPD) Gabriel Martinez, DHS NPPD	C) Relevant CyDentity Theme(s) – Check one or more <input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input type="checkbox"/> Provenance for the "Internet of Things" <input checked="" type="checkbox"/> Metrics for Trust <input checked="" type="checkbox"/> Other (please describe briefly) – adds benefit analysis to "trust"
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Provide a framework (visual, graphical) that addresses the problem of low risk, benefit, and trust impact decisions on context-dependent access control and determine actions in dynamic environments to drive control decisions. Ex: first responder ad-hoc networks need to evolve over time.	E) Outline of Research Concept Proposed; What's New About it? Framework will allow for dynamic optimization and decision making as risk, benefit, trust, and context evolve. Current systems are static, based on pre-defined models of risk and do not incorporate feedback of actions taken after access.
F) Which Disciplines are Necessary to Conduct the Research? Computer science Security Operations research Data visualization	G) How Will You Evaluate Progress and Measure Effectiveness? Milestone 1: establishing framework for these relationships. Milestone 2: identifying use of framework in an optimization/decision support context.
H) What research timeframe will be needed to address this Research Concept? <input type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential "risks" associated with this approach? Framework cannot be adequately established.

TEMPLATE 2: DISTRIBUTED EVALUATION / ESTIMATION OF TRUST

Authors: Egan, Wright, Roth, Jain

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	ID Proofing	Theme 1: Provenance	Theme 2: Metrics of Trust	Other	Authentication	Risk	Data and Application	Access	User Experience	Other
2	Distributed Evaluation / Estimation of Trust	X	X	X			X				

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name: Distributed Evaluation / Estimation of Trust	
B) Contributing Participants and Kibitzers: Dennis Egan, Rutgers University Rebecca Wright, Rutgers University Dan Roth, UIUC Ashish Jain, iConnective	C) Relevant CyDentity Theme(s) – Check one or more <input checked="" type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input checked="" type="checkbox"/> Provenance for the “Internet of Things” <input checked="" type="checkbox"/> Metrics for Trust <input type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. A distributed system of parties, in support of generating a system-wide, emerging trustworthiness in the individuals.	E) Outline of Research Concept Proposed; What’s New About it? Trust is an approximation of some truths. Level of approximation tradeoffs, risk and privacy Build a functional prototype Perform some experiments designed to evaluate
F) Which Disciplines are Necessary to Conduct the Research? Computer science Machine learning Computational social sciences	G) How Will You Evaluate Progress and Measure Effectiveness? Benchmark it with the existing reputation / risk scoring systems
H) What research timeframe will be needed to address this Research Concept? <input checked="" type="checkbox"/> Short term (1-2 years) <input type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential “risks” associated with this approach? Aggregation approach may not converge Getting data / participation due to proprietary issues

TEMPLATE 3: SOCIAL THINGS: SELF-ORGANIZING NETWORKS OF TRUST FOR THE INTERNET OF THINGS

Authors: Windley, Fefferman

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
3	Social Things: Self-Organizing Networks of Trust for the IoT		X				X				

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name: Social Things: Self-Organizing Networks of Trust for the IoT	
B) Contributing Participants and Kibitzers: Phil Windley, BYU Nina Fefferman, Rutgers University	C) Relevant CyDentity Theme(s) – Check one or more <input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input checked="" type="checkbox"/> Provenance for the "Internet of Things" <input type="checkbox"/> Metrics for Trust <input type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Current approach to IoT networks is static and based on apriori-determined topology. Resilient IoT will require dynamic grouping and organization of devices. Ex: new electric car needs to negotiate charging times with air conditioner and TV to avoid higher electric bill. How do existing devices learn to trust the car?	E) Outline of Research Concept Proposed; What's New About it? Research uses existing testbed for modeling network of connected smart devices to experiment with device/group discovery, dynamic group formation based on trust building and reputation. Reputation based on device attributes and provenance including transaction history. Devices expect and mitigate failure and exhibit resilience to anomalous behavior. Research increases overall security of IoT networks by exploring networks that are resilient to anomalous events rather than merely trying to prevent it.
F) Which Disciplines are Necessary to Conduct the Research? Distributed computing Device engineering System modeling Identity and reputation Machine learning Mathematics of self-organizing systems	G) How Will You Evaluate Progress and Measure Effectiveness? Create systems that self-organize according to discovery, reputation and decision making algorithms. Use "chaos monkey" to randomly inject byzantine faults and evaluate ability of networks to respond to failure and anomalies, as well as "heal" after any excursion.
H) What research timeframe will be needed to address this Research Concept? <input type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential "risks" associated with this approach? May miss global solutions due to getting caught in local minima.

EXPOSURES

Authors: Fefferman, Egan, Jain, Wright

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
4	Free Market Economy Based Attribution of Cyber Risk Exposures			X			X				

CYDENTITY RESEARCH CONCEPT TEMPLATE

<p>A) Proposed Research Concept Name: Free Market Economy Based Attribution of Cyber Risk Exposures</p>	
<p>B) Contributing Participants and Kibitzers: Nina Fefferman, Rutgers University Dennis Egan, Rutgers University Ashish Jain, iConnective Rebecca Wright, Rutgers University</p>	<p>C) Relevant CyDentity Theme(s) – Check one or more</p> <p><input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches</p> <p><input type="checkbox"/> Provenance for the “Internet of Things”</p> <p><input checked="" type="checkbox"/> Metrics for Trust</p> <p><input type="checkbox"/> Other (please describe briefly)</p>
<p>D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible.</p> <p>No existing way to relate industry best practices to cyber risk. Cyber risk cannot be priced currently. Cyber risk pricing is a second-order effect, depending on perception, i.e. low prices for insurance suggests low risk.</p>	<p>E) Outline of Research Concept Proposed; What’s New About it?</p> <p>Crowd-sourced gamification to estimate risk pricing. Create a virtual marketplace and use simulated and real cyber events to observe changes in how cyber risk is evaluated.</p>
<p>F) Which Disciplines are Necessary to Conduct the Research?</p> <p>Economy Gamification developers Portfolio managers IT security</p>	<p>G) How Will You Evaluate Progress and Measure Effectiveness?</p> <p>Benchmark against real cyber events after optimizing baseline data.</p>
<p>H) What research timeframe will be needed to address this Research Concept?</p> <p><input type="checkbox"/> Short term (1-2 years)</p> <p><input checked="" type="checkbox"/> Mid-term (3 years)</p> <p><input type="checkbox"/> Long-term (5 years)</p>	<p>I) What are the potential “risks” associated with this approach?</p> <p>Bootstrapping the game. No control over really rare events that could alter the marketplace but do not occur during period of performance.</p>

TEMPLATE 5: CATAPULTING LAW ENFORCEMENT INVESTIGATIONS INTO THE WORLD OF CYBERCRIME

Author: Pottenger

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access	User Experience	Other
5	Catapulting Law Enforcement Investigations into the World of Cybercrime	X			X		X				

CYDENTITY RESEARCH CONCEPT TEMPLATE	
A) Proposed Research Concept Name: Catapulting Law Enforcement Investigations into the World of Cybercrime	
B) Contributing Participants and Kibitzers: Bill Pottenger, Intuidex, Inc. and CCICADA COE	C) Relevant CyDentity Theme(s) – Check one or more <input checked="" type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input type="checkbox"/> Provenance for the "Internet of Things" <input type="checkbox"/> Metrics for Trust <input checked="" type="checkbox"/> Other (please describe briefly) - Transition to Law Enforcement
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Technology adoption is challenging, especially in law enforcement. Rolling out additional cybercrimes investigative capabilities to an existing platform in use by law enforcement will facilitate adoption.	E) Outline of Research Concept Proposed; What's New About it? This is a "catapult" concept. It represents a unique opportunity to put the investigation of financial and related cybercrimes within the grasp of law enforcement, including federal, state, and local, using advanced analytics, including data sharing.
F) Which Disciplines are Necessary to Conduct the Research? Data analytics in law enforcement	G) How Will You Evaluate Progress and Measure Effectiveness? Rate of adoption Delta in number of cases solved Intuidex, Inc. will enable distribution of sophisticated cyber analytics, developed by COEs like CCICADA for investigation of financial and related cybercrimes to law enforcement worldwide through its Watchman Analytics platform.
H) What research timeframe will be needed to address this Research Concept? <input type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential "risks" associated with this approach? Bridging the gap to bring COE technology up to commercial standards.

TEMPLATE 6: BOOTSTRAPPING IDENTITY

Authors: Sharkey, Pandey, Wullert, Martinez

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
6	Bootstrapping Identity	X	X	X		X	X				

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name: Bootstrapping Identity	
B) Contributing Participants and Kibitzers: Thomas Sharkey, RPI Anshul Vikram, NYU Graduate Student John Wullert, Leidos (support to DHS NPPD) Gabriel Martinez, DHS NPPD	C) Relevant CyDentity Theme(s) – Check one or more <input checked="" type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input checked="" type="checkbox"/> Provenance for the "Internet of Things" <input checked="" type="checkbox"/> Metrics for Trust <input type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. There are many situations where an identity must be applied or transferred to a new device, used as purchase of new IoT, or opening of new account. How can various identifiers, behaviors and attributes be combined to create sufficient ID confidence for a task at hand.	E) Outline of Research Concept Proposed; What's New About it? Application of multiple dimensions of identifying information to create a limited identity (user knowledge (PIN), user behavior, etc.). Investigate analogies/similarities to self-organizing IoT and "thin-file" identity creation.
F) Which Disciplines are Necessary to Conduct the Research? Cybersecurity Operations research Computer science	G) How Will You Evaluate Progress and Measure Effectiveness? Crowdsourcing could be used as a means of data collection of user trust assessments.
H) What research timeframe will be needed to address this Research Concept? <input type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential "risks" associated with this approach? Commercial solutions evolve to create complex web of incompatible solutions.

TEMPLATE 7: LIMITED LIABILITY PERSONA: BRINGING THE CONCEPT TO LIFE

Authors: Kaliya, Gebel

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access	User Experience	Other
7	Limited Liability Persona: Bringing the Concept to Life	X		X			X				

CYDENTITY RESEARCH CONCEPT TEMPLATE	
A) Proposed Research Concept Name: Limited Liability Persona: Bringing the Concept to Life	
B) Contributing Participants and Kibitzers: Kaliya, Leola Group Gerry Gebel, Axiomatics Americas	C) Relevant CyDentity Theme(s) – Check one or more <input checked="" type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input type="checkbox"/> Provenance for the "Internet of Things" <input checked="" type="checkbox"/> Metrics for Trust <input type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Corporate entities have a number of legal protections that are not currently available to individuals in online interactions. LLP establishes the principle of a legal entity that is comprised of financial constraints as well as identity constraints for use in different contexts.	E) Outline of Research Concept Proposed; What's New About it? Rather than a complete outline, here are some characteristics: <ul style="list-style-type: none"> • LLPs are a highly proofed ID without using weak KBA technologies. They are government sanctioned and approved. • Consumers choose financial limited and identity attribution and can create multiple LLPs • Relying parties can trust LLPs to a greater degree due to its provenance characteristics
F) Which Disciplines are Necessary to Conduct the Research? Legal review of concepts Technical review of LLP constructs Social review of acceptability	G) How Will You Evaluate Progress and Measure Effectiveness? <ul style="list-style-type: none"> • Measure growth in number of LLPs issued (could have multiple per person) • Measure growth of issuing parties • Measure growth of relying parties that accept LLPs
H) What research timeframe will be needed to address this Research Concept? <input checked="" type="checkbox"/> Short term (1-2 years) <input type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential "risks" associated with this approach? <ul style="list-style-type: none"> • Consumers don't accept • Relying parties insist on having more data on users

TEMPLATE 8: ALLOWABLE STATEMENTS USING METRICS OF TRUST

Authors: Roberts

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
8	Allowable Statements Using Metrics of Trust			X			X				

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name: Allowable Statements Using Metrics of Trust	
B) Contributing Participants and Kibitzers: Fred Roberts, Rutgers University	C) Relevant CyDentity Theme(s) – Check one or more <input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input type="checkbox"/> Provenance for the "Internet of Things" <input checked="" type="checkbox"/> Metrics for Trust <input type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Metrics are needed for trust. Before we can develop metrics for trust, we need to have an idea of how they will be used. One component of this is the statements we will want to be able to make using them especially if trust is more than binary (trusted or not trusted). Do we want to be able to say that X is twice as trustworthy as Y? If trust is like weight, we can say X is two times as trustworthy as Y because this is true in lbs and kgs. But this is not the same if trust is like temperature when there is the possibility of changing zero point as well as unit. And current not the case if trust is a rule from 1 to 5 or green, yellow, red. Do we want to say trustworthiness of X is reaching a threshold?	E) Outline of Research Concept Proposed; What's New About it? Research challenges: what kinds of metrics for trust need to be able to make what kinds of statements? How do we bring uncertainty into the picture? Is there a probabilistic version of such statements? What kinds of imaging/composing processes can we use? These kinds of issues as well studied in economics, psychology, ecology, epidemiology, psychophysics, etc. but I don't know of a literature on trust. Should work with existing efforts such as vectors of trust.
F) Which Disciplines are Necessary to Conduct the Research? Metrology Theory of Measurement Mix of Math, Logic, and Psych ECE / CS	G) How Will You Evaluate Progress and Measure Effectiveness? This is a front end to most work in trust metrics. The process is measureable by extend to which it influences discretion of new aspects on trust metrics.
H) What research timeframe will be needed to address this Research Concept? <input checked="" type="checkbox"/> Short term (1-2 years) <input type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential "risks" associated with this approach? Researchers in trust may not pay attention. We won't have enough examples of trust metrics to help develop.

TEMPLATE 9: IDENTITY ORACLE: PROOFING/AUTHENTICATION AGAINST ONE'S OWN BEHAVIOR, BIOMETRIC AND OTHER DATA

Authors: Kaliya

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access	User Experience	Other
9	Identity Oracle: Proofing/Authentication against one's own behavior, biometric and other data	X				X					

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name:

Identity Oracle: Proofing/Authentication against one's own behavior, biometric and other data

B) Contributing Participants and Kibitzers:

Kaliya, Leola Group

C) Relevant CyDentity Theme(s) – Check one or more

- ☒ Identity Proofing in the Era of Social Media and Data Breaches
- ☐ Provenance for the "Internet of Things"
- ☐ Metrics for Trust
- ☐ Other (please describe briefly)

D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible.

If behavior data matters in proofing how individuals collect their own data train from their devices. How can this be used to support self-authentication vs. data bank/store/vault?

E) Outline of Research Concept Proposed; What's New About it?

Working with technical folks we actually build prototypes to collect data and implement to understand if it is possible. My own geolocation relative historic pattern. My own biometrics in my own store of them.

F) Which Disciplines are Necessary to Conduct the Research?

Computer science
Enterprise IdM

G) How Will You Evaluate Progress and Measure Effectiveness?

Working prototype integrated and productized. Could be used in multi-party crypto computing.

H) What research timeframe will be needed to address this Research Concept?

- ☐ Short term (1-2 years)
- ☒ Mid-term (3 years)
- ☐ Long-term (5 years)

I) What are the potential "risks" associated with this approach?

Creates a big vulnerability for an individual. Reduces what can be stolen in whole database.

PROOFING

Authors: Best, Cowell, Maciejewski, Cooper

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
10	Multi-Model Behavior Confidence Measurement for Identity Proofing	X		X		X	X				

CYDENTITY RESEARCH CONCEPT TEMPLATE	
A) Proposed Research Concept Name: Multi-Model Behavior Confidence Measurement for Identity Proofing	
B) Contributing Participants and Kibitzers: Daniel Best, PNNL; Andrew Cowell, PNNL; Ross Maciejewski, ASU; Jim Cooper, PANYNJ	C) Relevant CyDentity Theme(s) – Check one or more <input checked="" type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input type="checkbox"/> Provenance for the “Internet of Things” <input checked="" type="checkbox"/> Metrics for Trust <input type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Knowing when a person is behaving as they should for a given role and for their normal activities is a difficult problem. Having insight into deviations. ICS has this problem and needs a way to find indicators beyond the single analyst scale. Partners can bring previous work on models, immediate operational partner, and ability to use PNNL data for research.	E) Outline of Research Concept Proposed; What’s New About it? Build out initial PNNL research on behavior models for identity confidence, starting with one ICS type and move generalized models to the others. We propose having multiple models that help comprise an identity confidence score. That score can be used for automated sandboxing and elevating profiles. Identity confidence would also be tied to job function baseline to ensure activity is expected. Early work would include model research on how many models are needed for accurate confidence and how many people are needed for general job category profile models.
F) Which Disciplines are Necessary to Conduct the Research? Computer science Social-behavioral Modeling and simulation Visualization	G) How Will You Evaluate Progress and Measure Effectiveness? <ul style="list-style-type: none"> Can correlate to risk buy down in risk for CT aspect of critical infrastructure Timeliness of tech transfer Red team (self-appointed bad guy) to adjust behavior to see if they’re caught (with correct paperwork/authorities)
H) What research timeframe will be needed to address this Research Concept? <input checked="" type="checkbox"/> Short term (1-2 years) – investigation and development for single ICT partner <input checked="" type="checkbox"/> Mid-term (3 years) – application to other ICT partners <input checked="" type="checkbox"/> Long-term (5 years) – model steering	I) What are the potential “risks” associated with this approach? False positives can lead to fake accusations – however, mitigated by soft sandboxing.

TEMPLATE 11: SMARTCARD TECHNOLOGY TO BE USED IN DRIVERS LICENSES: COST BENEFIT ASSESSMENT TO SOCIETY

Authors: Nolan, Wullert, Martinez

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
11	Smartcard Technology to be used in Drivers Licenses: cost benefit assessment to society	X	X	X		X					

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name:

Smartcard Technology to be used in Drivers Licenses: cost benefit assessment to society

B) Contributing Participants and Kibitzers:

Dave Nolan, DHS NPPD
John Wullert, Leidos (support to DHS NPPD)
Gabriel Martinez, DHS NPPD

C) Relevant CyDentity Theme(s) – Check one or more

- ☒ Identity Proofing in the Era of Social Media and Data Breaches
☒ Provenance for the "Internet of Things"
☒ Metrics for Trust
☐ Other (please describe briefly)

D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible.

A cost benefit to the individual from a privacy perspective, and opportunities to business for a standard trust source. Leverage centralized identifiers for distributed and mobile user authorization.

E) Outline of Research Concept Proposed; What's New About it?

Examine existing examples and emerging cases of State government issue of electronic identifiers and evaluate costs, benefits, and risks. Explore both government and business applications of this potential next generation of critical infrastructure.

F) Which Disciplines are Necessary to Conduct the Research?

Economics
Sociology
Legal / liability expert
Identity and identity management

G) How Will You Evaluate Progress and Measure Effectiveness?

Understanding of existing motivations for deployment. Use cases, benefits, and risks described in a white paper.

H) What research timeframe will be needed to address this Research Concept?

- ☒ Short term (1-2 years)
☐ Mid-term (3 years)
☐ Long-term (5 years)

I) What are the potential "risks" associated with this approach?

Minimal

TEMPLATE 12: TRANSPARENCY OF FEDERATION HUBS

Authors: Simonsen, Manz

Concept		CyIdentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
12	Transparency of Federation Hubs			X	X	X			X		

CYDENTITY RESEARCH CONCEPT TEMPLATE	
A) Proposed Research Concept Name: Transparency of Federation Hubs	
B) Contributing Participants and Kibitzers: David Simonsen, WAYF.DK David Manz, PNNL	C) Relevant CyIdentity Theme(s) – Check one or more <input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input type="checkbox"/> Provenance for the "Internet of Things" <input checked="" type="checkbox"/> Metrics for Trust <input checked="" type="checkbox"/> Other (please describe briefly) - usability
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. (In)visibility of federation hubs (i.e. user consent, branding).	E) Outline of Research Concept Proposed; What's New About it? Additional functionality for IdP and fed-hub. Transparency of the hub. Less imposition on the end user of the hub.
F) Which Disciplines are Necessary to Conduct the Research? Privacy experts Infrastructure architecture Usability experts	G) How Will You Evaluate Progress and Measure Effectiveness? Usability testing Transparency trusting Adoption Benchmark against present baseline
H) What research timeframe will be needed to address this Research Concept? <input checked="" type="checkbox"/> Short term (1-2 years) <input type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential "risks" associated with this approach? Misleading user management role of hub. No better than status quo.

TEMPLATE 13: IDENTITY MANAGEMENT IN SUPPORT OF TELECOMMUNICATIONS SERVICES AUTHORIZATION FOR EMERGENCY COMMUNICATIONS

Authors: Nolan, Wullert, Martinez, Cooper

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
13	Identity Management in Support of Telecommunications Services Authorization for Emergency Communications	X	X			X			X		

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name: Identity Management in Support of Telecommunications Services Authorization for Emergency Communications	
B) Contributing Participants and Kibitzers: Dave Nolan, DHS NPPD John Wullert, Leidos (support to DHS NPPD) Gabriel Martinez, DHS NPPD Jim Cooper, PANYNJ	C) Relevant CyDentity Theme(s) – Check one or more <input checked="" type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input checked="" type="checkbox"/> Provenance for the "Internet of Things" <input type="checkbox"/> Metrics for Trust <input type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Traffic characteristics needed to identify prioritization and quality of services (QOS) are obscured or not available to network operators, and critical communication could fail during emergency events.	E) Outline of Research Concept Proposed; What's New About it? Study LTE cellular networks. Prioritization and QOS and define the required identity management attributes needed to assure properly transmitted critical traffic during crisis situations. Demonstrate in lab trial techniques.
F) Which Disciplines are Necessary to Conduct the Research? Telecommunications Cybersecurity Emergency management	G) How Will You Evaluate Progress and Measure Effectiveness? Establish lab trial milestones and conduct trials, evaluate results and repeat.
H) What research timeframe will be needed to address this Research Concept? <input checked="" type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential "risks" associated with this approach? Duplication of effort with FirstNet

TEMPLATE 14: IDENTITY FOR ACCESS TO CRITICAL COMMUNICATIONS DURING CRISIS

Authors: Nolan, Wullert, Martinez, Queralt

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
14	Identity for Access to Critical Communications during Crisis				X	X			X		

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name: Identity for Access to Critical Communications during Crisis	
B) Contributing Participants and Kibitzers: David Nolan, DHS NPPD John Wullert, Leidos (support to DHS NPPD) Michael Queralt, Queralt, Inc Gabriel Martinez, DHS NPPD	C) Relevant CyDentity Theme(s) – Check one or more <input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input type="checkbox"/> Provenance for the “Internet of Things” <input type="checkbox"/> Metrics for Trust <input checked="" type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. During incident management, identities of responders need to be verified and role-based resources need to be assigned within NIMS environment.	E) Outline of Research Concept Proposed; What’s New About it? Investigate identify schemes, containers, etc. necessary to assign resources (telecom) in an actionable/timely means. Work with DHS S&T (Karyn Higa-Smith) and FEMA to leverage PIV-I attribute creation from emergency management.
F) Which Disciplines are Necessary to Conduct the Research? Telecom Cybersecurity Emergency Management	G) How Will You Evaluate Progress and Measure Effectiveness? Standards for PIV-I attributes/containers for emergency management. Demonstration in laboratory environment.
H) What research timeframe will be needed to address this Research Concept? <input checked="" type="checkbox"/> Short term (1-2 years) <input type="checkbox"/> Mid-term (3 years) Long-term (5 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential “risks” associated with this approach? Coordination with FirstNet.

TEMPLATE 15: SHORT TEXT PROACTIVE AUTHENTICATION

Authors: Roth

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
15	Short Text Proactive Authentication	X	X			X					

CYDENTITY RESEARCH CONCEPT TEMPLATE	
A) Proposed Research Concept Name: Short Text Proactive Authentication	
B) Contributing Participants and Kibitzers: Dan Roth, UIUC	C) Relevant CyDentity Theme(s) – Check one or more <input checked="" type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input checked="" type="checkbox"/> Provenance for the “Internet of Things” <input type="checkbox"/> Metrics for Trust <input type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Facilitate authentication on mobile devices using very short pieces of contributed text.	E) Outline of Research Concept Proposed; What’s New About it? The machine learning based technology will be based on two key innovations: 1) The ability to sense multiple features of the way the input text is being key-ed in (speed, rate, gaps, etc.) 2) The input sequence will be requested by the device in a specific way (rather than chosen by the user) 3) The device may introduce difficulties while the input sequence is being entered by the user as a way to (i) surprise the user and (ii) enlarge the input space. A machine learning algorithm will map this to a unique signature
F) Which Disciplines are Necessary to Conduct the Research? Computer science Machine learning	G) How Will You Evaluate Progress and Measure Effectiveness? Datasets will be generated to evaluate the quality of the authentication with multiple users, friendly and adversarial.
H) What research timeframe will be needed to address this Research Concept? <input type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential “risks” associated with this approach? The technology does not exist but we have relevant theory and related experiments.

TEMPLATE 16: ENABLING SOCIAL MEDIA CONSUMERS TO UNDERSTAND PRIVACY RISKS

Authors: Maciejewski, Powell, Best

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
16	Enabling Social Media Consumers to Understand Privacy Risks	X					X			X	

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name: Enabling Social Media Consumers to Understand Privacy Risks	
B) Contributing Participants and Kibitzers: Ross Maciejewski, Arizona State University Andrew Powell, PNNL Daniel Best, PNNL	C) Relevant CyDentity Theme(s) – Check one or more <input checked="" type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input type="checkbox"/> Provenance for the "Internet of Things" <input type="checkbox"/> Metrics for Trust <input type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Social media consumers are often unaware of the privacy implications of info given away in their blogs, tweets, etc., particularly in the context of how linking seemingly private data can allow identity/information discovery. What we mean is that if researcher link publically available datasets they can often extract context relevant information on identity.	E) Outline of Research Concept Proposed; What's New About it? Our goal is to explore common security questions and enable users to mine their own publically available data to assign privacy risk measurements to their own social media profiles. What's new is we want to not be data collectors, but privacy analysts that put a public portal forward to advocate social media users about risks related to their practices. What KBA statements might be most publically exposed?
F) Which Disciplines are Necessary to Conduct the Research? Computer science Graph analytics Psychology	G) How Will You Evaluate Progress and Measure Effectiveness? 1) Develop tools to scrape profile, plus text analysis 2) Metric to assign risk 3) Evaluate metric with various profiles 4) User study to see how this information relates to user experience
H) What research timeframe will be needed to address this Research Concept? <input type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential "risks" associated with this approach? May find consumers don't care or that are burnt out or feel powerless about this issue.

TEMPLATE 17: TRANSACTION HISTORY OF TRUSTED 3RD PARTY / INTERMEDIATE OPERATIONS

Authors: Simonsen, Manz

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
17	Transaction History of Trusted 3rd Party / Intermediate Operations		X	X				X		X	

CYDENTITY RESEARCH CONCEPT TEMPLATE	
A) Proposed Research Concept Name: Transaction History of Trusted 3 rd Party / Intermediate Operations	
B) Contributing Participants and Kibitzers: David Simonsen, WAYF.DK David Manz, PNNL	C) Relevant CyDentity Theme(s) – Check one or more <input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input checked="" type="checkbox"/> Provenance for the "Internet of Things" <input checked="" type="checkbox"/> Metrics for Trust <input type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Transaction History of Trusted 3 rd Party / Intermediate Operations	E) Outline of Research Concept Proposed; What's New About it? The right to be forgotten. Non-repudiability of transactions. Articulation of need for detection, respecting jurisdictional requirements.
F) Which Disciplines are Necessary to Conduct the Research? Legal experts – data storage and privacy Infrastructure architects	G) How Will You Evaluate Progress and Measure Effectiveness? Appropriate validation of performance requirements (see E). Compare against status quo.
H) What research timeframe will be needed to address this Research Concept? <input checked="" type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential "risks" associated with this approach? Retaining too much information or too little.

TEMPLATE 18: A VISUAL ANALYTIC APPROACH FOR ANALYSIS AND RESPONSE TO NAT AND IOT ATTACKS

Authors: Koven

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
18	A Visual Analytic Approach for Analysis and Response to NAT and IoT Attacks		X					X		X	

CYDENTITY RESEARCH CONCEPT TEMPLATE	
A) Proposed Research Concept Name: A Visual Analytic Approach for Analysis and Response to NAT and IoT Attacks	
B) Contributing Participants and Kibitzers: Jay Koven, NYU Graduate Student	C) Relevant CyDentity Theme(s) – Check one or more <input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input checked="" type="checkbox"/> Provenance for the “Internet of Things” <input type="checkbox"/> Metrics for Trust <input type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Real-time response to NAT attacks detected by existing early anomaly detection. To achieve this, we will develop a V.A. feedback loop with an operation in context of the response, while being assisted by intelligent analysis.	E) Outline of Research Concept Proposed; What’s New About it? Develop methods of visualization that will allow current systems to understand what is transpiring on their networks and helps them respond appropriately.
F) Which Disciplines are Necessary to Conduct the Research? Network, Visual Analytics, CHI, Machine Learning, and NAT domain expertise	G) How Will You Evaluate Progress and Measure Effectiveness? Create a NAT simulation and evaluate response to known and expected modes of attack
H) What research timeframe will be needed to address this Research Concept? <input type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential “risks” associated with this approach? Lack of acceptance, lack of domain expertise interaction

TEMPLATE 19: DIGITAL TRANSFORMATION INNOVATION LABORATORY

Authors: Brennan, Diener, Ho, Kantor

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
19	Digital Transformation Innovation Laboratory	X	X	X	X						X

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name: Digital Transformation Innovation Laboratory	
B) Contributing Participants and Kibitzers: Joni Brennan, Kantara Initiative Debra Diener, Independent Consultant Fenton Ho, TBS Canada Paul Kantor, Rutgers University	C) Relevant CyDentity Theme(s) – Check one or more <input checked="" type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input checked="" type="checkbox"/> Provenance for the “Internet of Things” <input checked="" type="checkbox"/> Metrics for Trust <input checked="" type="checkbox"/> Other (please describe briefly) – Tech Governance
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. While there are unique challenges by jurisdiction and business vertical, IoT is global, international security is global, business is global. Compare acceptable practice for global baselines. Test remote proofing solutions. Specific focus will be given to business models to sustain the organization including membership and subscriptions. The organization must deliver real, global value.	E) Outline of Research Concept Proposed; What’s New About it? Distill the “whole” for global view of tech and policy interoperability. Develop ID and privacy governance research. Informs policy to develop “trusted” markets.
F) Which Disciplines are Necessary to Conduct the Research? Identity management Economics Access control / authentication Labs to verify tech for measureable data Policy expertise	G) How Will You Evaluate Progress and Measure Effectiveness? Year 1: alpha pilot projects. Engage agile “start up” approach Year 3: committed government customers Negative and positive actionable data
H) What research timeframe will be needed to address this Research Concept? <input type="checkbox"/> Short term (1-2 years) <input type="checkbox"/> Mid-term (3 years) <input checked="" type="checkbox"/> Long-term (5 years)	I) What are the potential “risks” associated with this approach? Broad in scope and will need a modular approach with phases, small measures of success.

TEMPLATE 20: LANDSCAPES AND FIELD GUIDES: SENSE MAKING FOR COLLABORATION AND PROJECTS RESEARCH

Authors: Kaliya, Diener

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
20	Landscapes and Field Guides: Sense Making for Collaboration and Projects Research									X	X

CYDENTITY RESEARCH CONCEPT TEMPLATE	
A) Proposed Research Concept Name: Landscapes and Field Guides: Sense Making for Collaboration and Projects Research	
B) Contributing Participants and Kibitzers: Kaliya, Leola Group Debra Diener, Independent Consultant	C) Relevant CyDentity Theme(s) – Check one or more <input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input type="checkbox"/> Provenance for the "Internet of Things" <input type="checkbox"/> Metrics for Trust <input checked="" type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Really grapple with the means of core concepts used in the field and flush out landscapes / field guides on each of them to facilitate shared understanding.	E) Outline of Research Concept Proposed; What's New About it? Work has already been done but more could be. "Trust", "security", "identity", "ecosystem", "framework", "proofing", "names" and the emergence of shared language.
F) Which Disciplines are Necessary to Conduct the Research? Ethnography Identity experts with broad knowledge	G) How Will You Evaluate Progress and Measure Effectiveness? Standards for PIV-I attributes/containers for emergency management. Demonstration in laboratory environment.
H) What research timeframe will be needed to address this Research Concept? <input checked="" type="checkbox"/> Short term (1-2 years) <input type="checkbox"/> Mid-term (3 years) Long-term (5 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential "risks" associated with this approach?

TEMPLATE 21: DIGITAL TORN DOLLAR

Authors: Diener, Kantor, Brennan, Ho, Thurman

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
21	Digital Torn Dollar	X		X	X			X			

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name: Digital Torn Dollar	
B) Contributing Participants and Kibitzers: Debra Diener, Independent Consultant Paul Kantor, Rutgers University Joni Brennan, Kantara Initiative Fenton Ho, TBS Canada Dave Thurman, PNNL	C) Relevant CyDentity Theme(s) – Check one or more <input checked="" type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input type="checkbox"/> Provenance for the “Internet of Things” <input checked="" type="checkbox"/> Metrics for Trust <input checked="" type="checkbox"/> Other (please describe briefly) - Cross cultural and global business interoperable model
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Work with low tech digital analog (such as cryptocurrency block chains) to assess the algorithmic and cultural acceptability – compare to “torn dollar” as used in “Hawallan” for clarifying transfer of sensitive HSE info, rather than money.	E) Outline of Research Concept Proposed; What’s New About it? Looking at both algorithmic and cross cultural acceptability of a law tech authentication (one time, disposable) as criteria for development and dissemination. Block chains may be expensive for uptake. Alternate distributed approaches (e.g. peer to peer). Least amount of personal data.
F) Which Disciplines are Necessary to Conduct the Research? IT Cryptology Anthropology Sociology Ethics Privacy expert Finance / commerce Government	G) How Will You Evaluate Progress and Measure Effectiveness? Year 1: if no surprising results, quit. Year 3: at least one pilot implementation producing useful data
H) What research timeframe will be needed to address this Research Concept? <input checked="" type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) <input checked="" type="checkbox"/> Long-term (5 years)	I) What are the potential “risks” associated with this approach? Failure to integrate disciplinary goals toward the single goal

TEMPLATE 22: CONTEXT, HISTORY, POWER, TRUST OF CYBERSPACE

Authors: Kaliya

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
22	Context, History, Power, Trust of Cyberspace	X	X		X						X

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name: Context, History, Power, Trust of Cyberspace	
B) Contributing Participants and Kibitzers: Kaliya, Leola Group	C) Relevant CyDentity Theme(s) – Check one or more <input checked="" type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input checked="" type="checkbox"/> Provenance for the "Internet of Things" <input type="checkbox"/> Metrics for Trust <input checked="" type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Not all populations "trust" government institutions systems and/or corporate systems of constructing ID formally.	E) Outline of Research Concept Proposed; What's New About it? Work to understand cultural norms/existing practices fears associated with new/existing systems. Consider: LGBTQ, Religion, woman, African American, disabled, youth, etc. populations. What rights and responsibilities need to be understood to build accountable systems?
F) Which Disciplines are Necessary to Conduct the Research? Ethnic/Womens Studies Sociology Human Computer Interaction	G) How Will You Evaluate Progress and Measure Effectiveness? How we measure these groups "trust", interact, and adopt systems.
H) What research timeframe will be needed to address this Research Concept? <input type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential "risks" associated with this approach? Answers not listened to. The answers are used to create more oppressive government systems.

TEMPLATE 23: INTERSECTING REALMS OF ADAPTIVE PROVENANCE

Authors: Rajagopalan, Fefferman

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
23	Intersecting Realms of Adaptive Provenance		X					X			

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name: Intersecting Realms of Adaptive Provenance	
B) Contributing Participants and Kibitzers: Raj Rajagopalan, Honeywell Nina Fefferman, Rutgers University	C) Relevant CyDentity Theme(s) – Check one or more <input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input checked="" type="checkbox"/> Provenance for the "Internet of Things" <input type="checkbox"/> Metrics for Trust <input type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Entities participate in multiple networks with possibly different provenance needs. Its participants, networks, and provenance needs change. How do individuals resolve conflicts, adapt continuously without compromising functional integrity?	E) Outline of Research Concept Proposed; What's New About it? Generalizing distributed anomaly detection to multiple scales of interaction. Auto-integration of new individuals to existing networks while maintaining efficacy of distributed decision making. Identity is a critical enabler to agile community formation.
F) Which Disciplines are Necessary to Conduct the Research? Distributed anomaly detection Collaborative trust Automated deployment and configuration	G) How Will You Evaluate Progress and Measure Effectiveness? Ability to scale from networks with hundreds of nodes to networks with millions of nodes (meso-scale), while maintaining established benchmarks of distributed decision making effectiveness. There is a potential commercial interest in this, with different meso-scale structures.
H) What research timeframe will be needed to address this Research Concept? <input type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential "risks" associated with this approach? Formation and persistence of silos of functionality and security

TEMPLATE 24: COMBINED WITH 15

Authors: see 15

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
24	Combined with 15										

TEMPLATE 25: BLINDED 3RD PARTY (FEDERATION HUB)

Authors: Simonsen, Manz, Ho

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
25	Blinded 3rd Party (Federation Hub)			X	X			X			X

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name: Blinded 3 rd Party (Federation Hub)	
B) Contributing Participants and Kibitzers: David Simonsen, Danish e-Infrastructure Cooperation David Manz, PNNL Fenton Ho, Canada TBS	C) Relevant CyDentity Theme(s) – Check one or more <input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input type="checkbox"/> Provenance for the “Internet of Things” <input checked="" type="checkbox"/> Metrics for Trust <input checked="" type="checkbox"/> Other (please describe briefly) – Architecture
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Lack of trust in 3 rd party, insecure operation. Cryptographically securing and maintaining operations.	E) Outline of Research Concept Proposed; What’s New About it? Today, 3 rd parties work in clear text. We propose blinding them. No browser plug-ins should be required.
F) Which Disciplines are Necessary to Conduct the Research? Cybersecurity IT architecture Cryptography	G) How Will You Evaluate Progress and Measure Effectiveness? Test the “blindness” of the hub. Compare available functionality with today’s systems.
H) What research timeframe will be needed to address this Research Concept? <input type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential “risks” associated with this approach? Performance Encrypting too much/too little Loss of protocol independence

TEMPLATE 26: LEVERAGING FEDERATION HUBS FOR NON-WEB

Authors: Manz, Simonsen

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
26	Leveraging Federation Hubs for Non-Web		X					X			

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name: Leveraging Federation Hubs for Non-Web	
B) Contributing Participants and Kibitzers: David Manz, PNNL David Simonsen, Danish e-Infrastructure Cooperation	C) Relevant CyDentity Theme(s) – Check one or more <input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input checked="" type="checkbox"/> Provenance for the “Internet of Things” <input type="checkbox"/> Metrics for Trust <input type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Non-web federated access management	E) Outline of Research Concept Proposed; What’s New About it? Leverage federation hubs. Survey of non-web technologies. Integration and extension of non-web technology. Pilot of initial proof of principle.
F) Which Disciplines are Necessary to Conduct the Research? Security researchers IT/IdM infrastructure architects Non-web domain expert (IoT, SCADA, HPC...)	G) How Will You Evaluate Progress and Measure Effectiveness? Number of domains and adoption into operational settings
H) What research timeframe will be needed to address this Research Concept? <input type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) Long-term (5 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential “risks” associated with this approach? Increase in complexity Decrease in security Scalability concerns

TEMPLATE 27: AUGMENTED TRUSTED 3RD PARTY WITH SECURITY NOTIFICATIONS

Authors: Manz, Simonsen, Nash

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
27	Augmented Trusted 3rd Party with Security Notifications	X		X				X			

CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name: Augmented Trusted 3 rd Party with Security Notifications	
B) Contributing Participants and Kibitzers: David Manz, PNNL David Simonsen, Danish e-Infrastructure Cooperation Andrew Nash, Conform	C) Relevant CyDentity Theme(s) – Check one or more <input checked="" type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input type="checkbox"/> Provenance for the "Internet of Things" <input checked="" type="checkbox"/> Metrics for Trust <input type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. Trusted 3 rd party provides limited / no security situation awareness.	E) Outline of Research Concept Proposed; What's New About it? Leveraging Conform's Shared Signals model for federation hub.
F) Which Disciplines are Necessary to Conduct the Research? Security Infrastructure	G) How Will You Evaluate Progress and Measure Effectiveness? Security testing / red teaming Performance testing
H) What research timeframe will be needed to address this Research Concept? <input type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) Long-term (5 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential "risks" associated with this approach? Greater complexity Increased attack

TEMPLATE 28: PERSONAL MANAGEMENT IN THE WILD

Authors: Kaliya

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
28	Personal Management in the Wild				X	X					

CYDENTITY RESEARCH CONCEPT TEMPLATE	
<p>A) Proposed Research Concept Name: Personal Management in the Wild</p>	
<p>B) Contributing Participants and Kibitzers: Kaliya, Leola Group + Ethnographers</p>	<p>C) Relevant CyDentity Theme(s) – Check one or more</p> <p><input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches</p> <p><input type="checkbox"/> Provenance for the "Internet of Things"</p> <p><input type="checkbox"/> Metrics for Trust</p> <p><input checked="" type="checkbox"/> Other (please describe briefly)</p>
<p>D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible.</p> <p>How do different people (inclusive of marginal groups) actually manage to keep separate personas? This can inform future system/device/UI design to enable easier personal management.</p>	<p>E) Outline of Research Concept Proposed; What's New About it?</p> <p>The research will work with subjects to document these personal management strategies employed "in the wild." Research could also be used to better understand adversaries.</p>
<p>F) Which Disciplines are Necessary to Conduct the Research?</p> <p>Ethnography CtH Contextual Privacy</p>	<p>G) How Will You Evaluate Progress and Measure Effectiveness?</p> <p>We have real world understanding of what people do.</p>
<p>H) What research timeframe will be needed to address this Research Concept?</p> <p><input checked="" type="checkbox"/> Short term (1-2 years)</p> <p><input checked="" type="checkbox"/> Mid-term (3 years) Long-term (5 years)</p> <p><input type="checkbox"/> Long-term (5 years)</p>	<p>I) What are the potential "risks" associated with this approach?</p>

TEMPLATE 29: GLOBAL SURVEY OF STATE TO CITIZEN ID (EID) SYSTEMS: A COMPARATIVE EID OPEN SOURCE RESEARCH PROJECT

Authors: Kaliya

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment					
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience	Other
29	Global Survey of State to Citizen ID (eID) systems: a comparative eID open source research project			X	X						X

CYDENTITY RESEARCH CONCEPT TEMPLATE	
A) Proposed Research Concept Name: Global Survey of State to Citizen ID (eID) systems: a comparative eID open source research project	
B) Contributing Participants and Kibitzers: Kaliya, Leola Group (Francisco and Karen Pourcore)	C) Relevant CyDentity Theme(s) – Check one or more <input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input type="checkbox"/> Provenance for the “Internet of Things” <input checked="" type="checkbox"/> Metrics for Trust <input checked="" type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. What are the qualities / characteristics of existing State ID systems? We have brainstormed 40 questions.	E) Outline of Research Concept Proposed; What’s New About it? Community effort to get the answers about different country’s systems to help make sense of the world and what’s happening in it.
F) Which Disciplines are Necessary to Conduct the Research? Community Management Broad Knowledge of Industry professionals globally	G) How Will You Evaluate Progress and Measure Effectiveness? We will have a survey of global eID and in understanding what is in operations and coming into operation. We have a full matrix of 40+ countries.
H) What research timeframe will be needed to address this Research Concept? <input checked="" type="checkbox"/> Short term (1-2 years) <input type="checkbox"/> Mid-term (3 years) Long-term (5 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential “risks” associated with this approach?

TEMPLATE 30: HOW DOES NATURE DO “IDENTITY”? APPLYING BIOMIMICRY TO KEY CONCEPTS OF TRUST, AUTHENTICATION, AND SECURITY

Authors: Kaliya

Concept		CyDentity Theme Alignment				IDAM Competency Areas Alignment				
#	Title	Theme 1: ID Proofing	Theme 2: Provenance	Theme 3: Metrics of Trust	Other	Authentication	Risk	Data and Application Security	Access control	User Experience
30	How does Nature do “Identity”? Applying Biomimicry to Key Concepts of Trust, Authentication, and Security				X					X

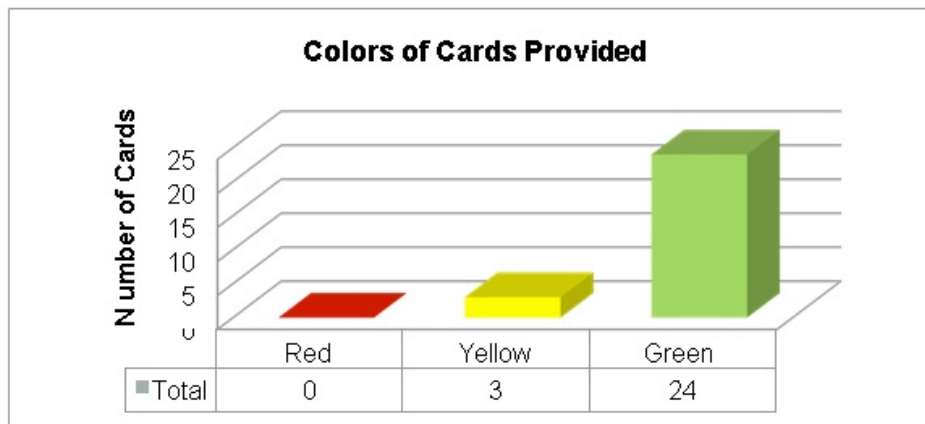
CYDENTITY RESEARCH CONCEPT TEMPLATE

A) Proposed Research Concept Name: How does Nature do “Identity”? Applying Biomimicry to Key Concepts of Trust, Authentication, and Security	
B) Contributing Participants and Kibitzers: Kaliya, Leola Group	C) Relevant CyDentity Theme(s) – Check one or more <input type="checkbox"/> Identity Proofing in the Era of Social Media and Data Breaches <input type="checkbox"/> Provenance for the “Internet of Things” <input type="checkbox"/> Metrics for Trust <input checked="" type="checkbox"/> Other (please describe briefly)
D) Brief Description of Problem Addressed by this Research Concept. Why is the Problem Difficult? Provide specific Instances or Concrete Examples of the Problem where possible. How does nature do it? This question has been asked by many a traditional field and a whole practice area / field called biomimicry has emerged.	E) Outline of Research Concept Proposed; What’s New About it? We could actively explore how natural systems “do” some of the key systems functions we are seeking to enable in socio-technical systems.
F) Which Disciplines are Necessary to Conduct the Research? Biomimicry (Biomimicry Inst.) Enterprise IDM professors	G) How Will You Evaluate Progress and Measure Effectiveness? We can learn new things
H) What research timeframe will be needed to address this Research Concept? <input type="checkbox"/> Short term (1-2 years) <input checked="" type="checkbox"/> Mid-term (3 years) <input type="checkbox"/> Long-term (5 years)	I) What are the potential “risks” associated with this approach? May be hard to find examples.

APPENDIX D: FEEDBACK AND LESSONS LEARNED

The CyDentity Sandpit facilitator used a method of red, yellow, and green cards to gather quick feedback from the participants at the end of the meeting. Each participant was asked to pick one card to anonymously give the sandpit project team feedback.

- Red Card: participant they did not get anything out of the meeting, meeting was unsuccessful
- Yellow Card: meeting was good, but there was room for lots of improvement
- Green Card: meeting was a great experience, learned a lot, and want to continue to stay involved in future discussions



If participants were inclined, they could provide specific feedback by writing on their card. The following is the written feedback received:

- No Red Card Feedback Received
- Yellow Card Feedback:
 - Great medium to get ideas and discussion worked out. More diversity needed in the provocateurs panel
 - Provide a wireless printer and/or email address so we could type and print our templates.
 - Would have liked greater participation from DHS personnel in attendance. More stage setting of the goals of the workshop would have been helpful. Greater collaboration should be encouraged, as many folks seemed to connect with those they already knew.
- Green Card Feedback
 - It would also be great to try this format but with a month between meeting and forming groups and when we pitch the (better formed) ideas. I realize it's hard to get the same folks to come twice.
 - Loved the broad range of participants from various domains. Have you spoken to DRDC Centre for Security Science? Had a number of conversations on IdM with them.
 - We could use more PhD students in the room for perspective.
 - Great workshop: good interaction, diversity, and kept it interesting through the duration. Can be improved: better preparation in terms of the backgrounds of other participants.
 - Definitely worth it. Very inspiring! Suggestion for easier group-forming: a round of 3 second pitches ahead of walk-through.
 - This was outstanding - terrific mix of background of the participants. The 1.5 days made for good, focused discussion. CyDentity 2 might focus on several of the projects that were selected based on this session. Rutgers setting was very conducive to the needed discussions.
 - Great meeting. Emily is brilliant.
 - Great. <3 Emily.
 - Excellent facilitation and coordination of sandpit. Quality of participants was high, though diversity (technical) was suspect. Saw some new collaborations form. More would have been better. Some people don't understand R&D purpose.
 - Great job in starting and moving forward and important conversation in very short time!

- Very good way to share and hear ideas. Good moderators to keep on time. Maybe need more time to get more collaboration integration.
- Useful and educational. A bit of warning about the 2-minute presentation might help.
- Great.
- Useful. Talks by the Provocateurs were nice. Very well organized. All hail Emily!
- How do we balance the advantages of homework and the spontaneity of collaboration face to face?
- Good balance/representation of academics, industry, and government. Panelists were well informed; aware of issues. Allocation of time to different parts of the process over 1.5 days was good. Tying "proposal" ideas to funding opportunity was key to stimulating engagement. Breakouts seemed less useful - clear objectives for them would help.
- Great program and great people. Enjoyed it and learned things.
- Excellent event. Well done.

Other feedback received (not on cards):

- Identity has been a disappointment for 20 years... finally getting excited about it again.
- Meet and greet event worked very well
- Needed a little bit more space
- 2 mins + 5 min Q&A worked very well, but consider: Give more time to prepare actual slides, presenter and note taker for each concept team, better to have earlier in the agenda
- Need more focused theme breakouts
- Opportunity to take things home would have been nice
- Could have a round robin at the end of Day 1 when concepts are submitted, then finalize presentations for the next day.
- Provocateurs:
 - High-level they agree on many things
 - Need to be more provoking, some controversial folks
 - They did challenge a bunch of notions
 - Maybe too much time on the agenda
 - Didn't kowtow to government biases
 - Need more diametrically opposed opinions across the panel (3D convo)
- Got enough out of discussion and concepts for 2-3 interesting projects for IDAM and CSD
- Challenge is to make sure projects are solving someone's pain; need to get expressions of interest that we are moving in the right direction from internal and external customers