LETTER REPORT

Priority Research Directions

Cyber Security Research Needs for Open Science

July 23-24 • Bethesda, Maryland

Submitted by Workshop Chairs

Patrick Burns[1], Susan Estrada[2] and George Michaels[3]

INTRODUCTION

This report contains preliminary results of Priority Research Directions (PRDs) identified during the two-day workshop titled *Cyber Security Research Needs for Open Science* held on July 23 and 24 at the Bethesda North Marriott Hotel. The invitation-only workshop was jointly sponsored by the DOE Office of Science and Office of Electricity Delivery and Energy Reliability. Nearly one hundred and fifty registered for the workshop and about one hundred and twenty-five attended. Participation included broad representation from national laboratories, higher education and industry. Participants self-identified their interests into five major break-out groups, each of which was charged with identifying PRDs.

WORKSHOP LOGISTICS

The workshop included plenary presentations from DOE program leaders and distinguished speakers from the field of Cyber Security: notably Steve Crocker from Shinkuro, George Spix from Microsoft, and Jason Stamp from Sandia National Laboratories. Presentations from these speakers informed the participants of the breakout groups, and motivated them to focus their attention on long-term research issues. Breakout sessions encompassed the following topics and leaders:

1. **Securing Hardware, Software and Data (SHSD)** – Len Napolitano[4] and Frank Siebenlist[5]
2. **Monitoring and Detection (MD)** – Troy Thompson[3] and John McHugh[6]
3. **Future Security Architectures and Information Assurance Technologies (FSA**) – Tom Harper[7]
4. **Human Factors Analysis (HF)** - Anne Schur[3] and Joe St Sauver[8]
5. **Protecting our Utility Infrastructure (UI)** – Jeff Dagle[3], Aaron Turner[7] and Bill Young[4]

---

[1] Colorado State University
[2] Aldea Communications
[3] Pacific Northwest National Laboratory
[4] Sandia National Laboratory
[5] Argonne National Laboratory
[6] Dalhousie University
[7] Idaho National Laboratory
[8] Internet2

Note that the session names are abbreviated in parentheses. These abbreviated names will be used subsequently in this report.

PRIORITY RESEARCH DIRECTIONS

All together, twenty-eight Priority Research Directions (PRDs) were identified independently in the sessions. However, a number of these have sufficient commonality that they were aggregated by the workshop chairs between and among sessions into seven overall thrust areas. The PRDs identified subsequently are organized into these seven thrust areas:

1. Open Science Security Architecture
2. Adaptive/Autonomic/Homeostatic Security and Response
3. Situational Awareness
4. Integrity and Pedigree
5. Usability, Characterization and Assessment
6. Control Systems
7. Future of Cryptography

After the final reports are prepared by the breakout session leaders and these content is subjected to additional scrutiny, these thrust areas may be further consolidated. That judgment will be made based on the details in each report.

RELEVANCE TO DOE'S OPEN SCIENCE AND ELECTRICITY DELIVERY AND ENERGY RELIABILITY ENVIRONMENTS

Protecting systems and users, while maintaining ease of access represents the "perfect storm" of challenges in the area of Cyber Security.

The charge to the workshop participants was to define PRDs relevant to DOE's open science and Electricity Delivery and Energy Reliability missions. Several distinctive factors pertinent to DOE's open science mission are: 1) access is required to expensive, centralized resources, 2) emphasis is "big science," and 3) users are highly decentralized and distributed and come from very diverse IT environments, most of which are not highly secured. Secretary of Energy Spencer Abraham described DOE's unique open science environment in a 2004 DOE report: "DOE's state-of-the-art facilities are shared with the science community worldwide and contain technologies and instrumentation that are available nowhere else. Each year, these facilities are used by more that 18,000 researchers from universities, other government agencies, private industry, and foreign nations."

With very expensive, one-of-a-kind hardware located around the world and with over 18,000 researchers needing access to the hardware, the data produced and the specialized computing resources that facilitate DOE's large worldwide collaborations, DOE is at a critical juncture. There is a clear need to provide new approaches and technologies to address Cyber Security in this environment. DOE needs flexible and scalable ways to provide a secure but usable scientific environment for its community of scientists and researchers. In addition, the nation's energy delivery infrastructure shares many of the same Cyber Security issues that exist in the open science environment, mandating an imperative for a synergistic, joint approach.

Each of the Office of Science divisions has determined strategic hardware needs for the next 20 years as described in the two reports: the *Office of Science Strategic Plan* and the *Facilities of the Future.* No matter which Office of Science division is examined, it is clear that their plans involve a significant need for strategic DOE computing and networking resources to allow their researchers to collaborate and to access strategic hardware. DOE researchers routinely use centralized, leadership-class computing resources (e.g. ANL, NERSC, ORNL and PNNL), decentralized processing capabilities, parallel computing facilities, massive data storage facilities and movement and sharing of data for use in analysis. The Office of Science's projection of new hardware and associated scientific endeavors for the next 5-10 years vastly expands the need for new Cyber Security research. One example is the near-term installation of the Large Hadron Collider where it is expected that researchers will need, at a minimum, tens of gigabits per second of network capacity to conduct their research effectively.

The Office of Electricity Delivery and Energy Reliability's report entitled *Roadmap to Secure Control Systems in the Energy Sector* further highlights the critical requirement for new Cyber Security research. Long-term efforts are needed to develop advanced materials and concepts for electricity delivery and storage to the US electric grid, assuring that it remains among the most robust, reliable, secure, and technologically advanced in the world. Improving the security of energy control systems is a crucial requirement to protect national infrastructure for energy delivery.

Improving Cyber Security is a complex, almost daunting task in both the open science and Control Systems environments. But with a focus on scalability and flexibility in the research directions, we and the attendees believe that significant forward progress toward creating both usable and secure environments can be made in the next ten years. The research directions suggested in this report will inspire new Cyber Security safeguards for both open science and Energy Control Systems.

It is additionally recognized that while the goal is to enable a secure and open science infrastructure for research, it is often the case that the mechanisms to deliver that security involve and overlap with classified operations for implementation. **It is imperative that the DOE Cyber infrastructure be effectively defended to ensure national energy security for the future.** Research in long-term science applicable to Cyber Security will have broad ranging value to the DOE mission as well as for National and Homeland Security.

The DOE Office of Science also has been driving the implementation of new, innovative Leadership Class Computing facilities and capacity. With a move to support exascale science and beyond, a new generation of computing technologies are emerging that will provide research opportunities for the next decade that could enable the development of intrinsically secure, information assured, open computing ecosystems. Many of those areas have been captured in the PRDs from this workshop.

The workshop produced innovative research directions that have the following attributes:

1. The PRDs represent significant challenges, requiring 3-10 years to address in a sustained research program.

2. Although many of the PRDs are the subject of research and development by other agencies, there are unique aspects to DOE's open science and energy control systems environments that merit new and different research and development by OASCR and OE.
3. The PRDs encompass numerous fundamental aspects of mathematics, algorithms and computational science.
4. The PRDs characterize research needed, and by and large, would take at least three years have to impact upon DOE's operational environments.
5. There are obvious synergies and overlap between Cyber Security in the open science environment and the energy control systems environment. The results of the research should eventually be applied to DOE's open science and the energy control systems environments, to render them both more secure and more accessible, leading to science conducted more efficiently and more effectively, and greater security, reliability and usability in the energy distribution environment.

PRIORITY RESEARCH DIRECTIONS

In this section, the PRDs will be individually presented in the aggregated thrust areas. Each PRD will be referenced to its original session. In this report, no attempt is made to condense or consolidate PRDs, so that the full details of the workshop are included.

1. Future Open Science Security Architecture

This thrust area involves understanding and developing a new, secure cyber architecture that can scale with forthcoming DOE open science requirements including extensive worldwide collaborations. The ultimate goal would be new capabilities and a set of baseline standards for Cyber Security that can be institutionalized by vendors.

"Security + Architecture = hard!"

a. **Open Science Security Architecture (FSA)** – This PRD involves developing a framework for integrating multi-site Cyber Security systems and components, and involves multi-level and multi-site interoperability and cooperation. Challenges involve the determination of an end-to-end security architecture (network, protocols, ID management, trust management, etc.) applicable in a large-scale, highly distributed environment. New Cyber Security discoveries include the development of standards and automation for secure exchange of security information, location, and time-aware authentication and authorization. Benefits of this research are greater understanding of Cyber Security from an end-to-end perspective, so that attention can be given to the current "weakest link." R&D in this area will facilitate broad, diverse, open science. The research is expected to require five to ten years to achieve fruition, although intermediate results may become available in three to five years.
b. **Trusted Virtualization (SHSD)** – This PRD involves developing a model for trusted virtualization of computational environments. Virtualization could provide a scalable computational ecosystem that would be based upon capabilities uncoupled from the hardware upon which software is deployed. Challenges involve extending trust from current hardware to emerging virtual environments, expressing and enforcing security goals at the level of a virtual machine, and maintaining Cyber Security when transitioning among virtual environments. New Cyber Security discoveries include the development of containment strategies, mechanisms for quantifiable verification of trust in virtual environments, and adding a Cyber Security layer to the virtual environment. Benefits of this research are greater

trust/Cyber Security in virtualized environments, greater efficiency of usage due to ability to load balance flexibly across and among virtual environments, and easier distribution and usability of software environments for the user. Additionally, this will address fault tolerant and resilient computing systems beyond petascale systems. The research is expected to require three to ten years to achieve fruition with advancements in computer science and mathematics.

c. **Economics-based Security Architecture (FSA)** – This PRD involves developing a model to analyze interactions between Cyber Security and user policies, phrase problems as sets of games, derive Nash equilibria, prove scalability, identify inflection points, and define countermeasures and associated costs. Challenges involve the uncertain and evolving black market economics associated with identity theft and system resources, inherent complexity, identification of security trade-offs, and determination of quantifiable model variables and parameters. New Cyber Security discoveries include the development of enforcement across multiple scales of heterogeneous systems, optimization of defense strategies, and a model with the capability to evaluate trade-offs in terms of hardware, network, software, policy and human countermeasures. The primary benefit of this research is a consistent understanding of all elements of Cyber Security that can be used to deploy resources (both human and machine) optimally. The research is expected to require three to ten years to achieve fruition.
d. **Cyber Security Information Framework for Open Science (SHSD)** – This PRD involves developing a new framework for assessing security in open science environments, including unifying the semantics of security data. Challenges involve the numerous complexities inherent in the open science environment – especially the multitude of different components, systems, sites and users. The framework must accommodate the complexity without impairing user accessibility and productivity, be scalable, and model appropriate trade-offs of Cyber Security against these areas. A self-consistent framework, in and of itself, would be a significant new Cyber Security discovery. The benefits of this research are more effective, trusted systems and greater integrity for use of those systems in distributed, open environments. It was not determined how long this research might take to achieve fruition.
e. **Resilient Distributed Computing (FSA)** – This PRD involves exploring a framework for fine-grained replication, replication on-demand, large-scale virtualization, and incremental migration as a means to assess, detect, and prevent the impact of loss or corruption of computational resources. Challenges involve incorporating replication into systems that are already running at or near capacity on very large science problems that may execute for extended periods of time. This problem is known to be canonically hard. New Cyber Security discoveries include the development of procedures to evaluate, distribute and (re)allocate computing resources in a highly distributed environment. R&D in this area will facilitate trust, increase availability (i.e. more cycles should become available) and enhance robustness in open science computing environments. The research is expected to require five to ten years to achieve fruition.
f. **Secure** S**oftware (SHSD)** – This PRD involves taking a fresh look at securing software, including detection, diagnosis, moderation and remediation of Cyber Security vulnerabilities. Challenges include the complexities of the diversity of software, distributed, heterogeneous systems upon which the software executes, the need for an end-to-and approach, and the long life cycles of some software. There are also human factors of how diagnostics, moderation, and remediation will be communicated to and interact with users, system administrators, and Cyber Security experts. New Cyber Security discoveries include parallel techniques for early

g. **Federated Cyber Security for Open Science (HF)** – This PRD addresses DOE's participation in the Internet2 federated identity management initiative. The DOE open science community has unique needs to provide secure and easy access to DOE resources – systems will be more secure and more accessible to the open science community. Challenges are that the open science community exists in a highly decentralized environment, involving many sites, each with different environments and policies for Cyber Security. New Cyber Security discoveries include novel techniques for user privilege negotiation among systems, user authentication, user authorization, and possibly remote configuration of cyber resources in the remote environment. Benefits of this research are better Cyber Security, easier accessibility to DOE resources, and distribution of the effort required to implement Cyber Security. The research is expected to require three to five years for initial efforts (federated authentication and authorization), and five to seven years for federated configuration.

2. Adaptive/Autonomic/Homeostatic Security and Response

The enormous complexity of computing systems in DOE open science and in energy control systems are, at times, beyond the capabilities of humans by themselves to assimilate and manage in real-time. Clearly sophisticated automated systems are required. This thrust area is focused on computer self-management of Cyber Security, based on human-defined policies and rules.

"An ounce of prevention is worth a pound of cure."

a. D**ecentralized Monitoring, Detection, and Response (human and automated) (MD)** – This PRD involves developing research methods and approaches for: dynamic modeling, triggers, proactive response mechanisms, and intelligent data reduction/analysis techniques including advanced visualization for analysts. Challenges are the need for a trusted link between the data and the human operator, characterization of data and data sets to be analyzed (e.g. systems, components, networks, users), coordinating and correlating across multiple decentralized domains, mitigating the effects of "poisoned" data, and the massive amount of data. New Cyber Security discoveries include development of self- and community-aware systems and next-generation systems that perform to DOE's requirements (ultra-high capacity and low latency). Benefits include improved Cyber Security in DOE systems, better decision support, and graceful degradation rather than catastrophic failure. The research is expected to require five to ten years to achieve fruition with advancements in computer science, new hardwired architectures, large-scale data intensive analytics and sensor developments.
b. **Autonomic Incident and Damage Containment (MD)** – This PRD involves developing secure approaches to autonomic Cyber Security incident and damage containment. The fields of control theory, group dynamics, machine learning and software assurance are involved. Challenges involve the size, speed, broad scope, and complexities inherent in the DOE open science environment. Benefits of this research are shorter time to identify and react to Cyber Security incidents, accomplished by removing or distancing the human from the system. How long this research might take to achieve fruition remains an open question due to the

rapid evolution and deployment of new technologies into communications and computing systems that continues to drive these systems to new performance levels and increase complexity.

3. Situational Awareness

Effective Cyber Security requires effective command, communications and control systems. Situational awareness is complex, dynamic and sometimes involves high-risk in DOE's open science and Energy environments. This thrust area focuses attention on understanding the situational complexity needed for effective Cyber Security including representations of objects, people, system states, interactions, environmental conditions and other situation-specific factors.

"The emphasis should be on MyScience instead of MySpace."

a. **Intrusion Prevention and Detection (FSA)** – This PRD involves developing a framework for analysis and characterization of the structure and nature of specific DOE open science data, control and execution paths. Methods and technologies are required to capture and process at extremely high speeds the following elements: monitoring, packet filtering, anomaly detection, information fusion, integrated response, fewer false positives, failback mechanisms, containment, and forensics. Challenges of this PRD are scale (extremely high traffic and number of users) and scope (vast geographical distribution and different types of systems). R&D in this area will improve trust among users and systems for broad, diverse, open science. The research is expected to require three to five years to achieve fruition, and production deployment may be achieved in four to ten years.
b. **Distributed Denial of Service (DDOS) tolerance (FSA)** – This PRD involves developing a focused examination of technology and techniques to defend large-scale, distributed computing and experimental systems against DDOS attacks while allowing the computation and/or experiment to continue. Challenges involve the development of vastly more sophisticated techniques and algorithms than are currently available. R&D in this area will promote safe, resilient computing and experiments in open science. The research is expected to require five to ten years to be put into production with advances in large-scale, data intensive network analytics and real-time automated network controls.
c. **Enabling Data and Code Sharing and Cooperative Analytics (MD)** – This PRD involves developing secure approaches to encourage users to greater degrees of sharing data, algorithms and applications. Challenges involve non-deterministic social factors, all of the difficulty inherent in data of different time and length scales in differing formats, and Cyber Security aspects. Benefits of this research are shorter time to solution and reduced storage and transmission capacity needs in the open science environment. This research is expected to require five to ten years to be put into production.
d. **Appropriate Distributed Defense (HF)** – This PRD involves research in techniques to query a wide variety of Cyber Security information sources that shield open science systems and users from known Cyber Security problems. Such sources might include databases and blacklists of known exploits, viruses, worms, malware, dangerous sites, etc. It is also proposed to develop an ecosystem-wide awareness capability, quantitative measures of the Cyber Security "health" of a system, and display results visually and intuitively in a real-time presentation suitable for program managers and security analysts. Challenges involve the size, speed, broad scope, and complexities inherent in the DOE open science environment. Benefits of this research are shorter time to identify and react to Cyber Security incidents as well as more comprehensive information about the health of a system to inform human

analysis and decision making. The research is expected to three years to begin to bear fruit, and five to ten years to be put fully into production.

4. Integrity and Pedigree

Today, DOE's scientists use a miasma of commercial off-the-shelf software in a blind trust model, including "software of uncertain pedigree" (SOUP). This thrust area develops the complex "back-ends" needed to define, measure, and make accessible to the science community integrity and pedigree.

a. **Long-term Integrity and Authenticity of Large and Dynamic Data Sets (FSA)** – This PRD involves developing data integrity models and analyses that: survive reductions/abstractions, accommodate privacy constraints, survive over the long-term, are auditable, are efficient in terms of processing, involve distributed, heterogeneous systems, and take into account uncertainty. Challenges are that data sets can be exceedingly large, involve aggregation/reduction/fusion, are often dynamic, and can persist over very long times. Techniques do not exist for measuring the integrity of data sets that are often the purview of distributed users and are not well understood by any individual. New Cyber Security discoveries in this area require fundamentally new approaches in analyzing, assessing and evaluating data, in error detection and correction, and in involving users in secure, effective behaviors. The research is expected to require five to seven years to achieve fruition.

b. **End-to-end Data Security (SHSD)** – This PRD involves developing new frameworks and techniques for end-to-end data security on distributed, heterogeneous systems. Challenges are managing storage and provenance for dynamic international collaborations for thousands of scientists across many, diverse platforms and domains. New Cyber Security discoveries in this area include automatic metadata capture, validation, and transfer among systems and users. This research is expected to result in more effective, trusted collaborations, and greater integrity for data in distributed environments. The research is expected to require five to ten years to achieve fruition.

c. **Secure Information Management (SHSD)** – This PRD involves developing new frameworks to protect critical information distributed across millions of nodes. Challenges are complexity and scalability: data sets can be exceedingly complex, large, data are often aggregated/reduced/fused, are often dynamic, can persist over very long times, and can exist on many, distributed, heterogeneous systems. Additionally, information involves much more than just data, including code (binary and source), metadata, and complex, sometimes unstructured relationships among data. New Cyber Security discoveries in this area require fundamentally new ontologies, models, processing approaches, and policies. This research is expected to result in more effective, trusted data and systems that will facilitate sharing data and resources among open science communities. The research is expected to require five to seven years initially to produce results and eight to ten years to achieve security and scalability.

d. **Verification of Intended Use (MD)** – This PRD involves developing new frameworks and methodologies to verify that both users of DOE open science systems and the applications run on them are as intended. New profiling application tools are needed to assure validation and verification of software for systems of the future. Research may span the areas of biometric devices, user usage and behavior (human "signatures") semantics, watermarking binary and source code, etc. Challenges involve complexities inherent with human factors,

the large-scale of traffic, large numbers of users, and complexity inherent in DOE open science distributed heterogeneous systems. New capabilities will be developed to detect human attacks, especially "insider" attacks, and enable more science by protecting systems from unintended use. The research is expected to require five to ten years to achieve fruition, although intermediate aspects may become available in seven to fifteen years.

5. Usability, Characterization and Assessment

Understanding the effect and affect of human behaviors in Cyber Security is imperative. To catalyze scientific discovery, a balance between usability and Cyber Security must exist, with an emphasis on usability. This thrust area provides for research in the primary understanding of human behavior both in launching attacks and in using Cyber Security in day-to-day work.

> *"In the Bentham calculus of protecting our systems, networks and data, the user is often forgotten, ignored, or even neglected, sometimes profoundly affecting productivity and impeding open science discoveries." – from the Human Factors session.*

a. **Characterization of Human Threats for Open Science (HF)** – This PRD involves developing scalable techniques to understand, predict, and detect human behavior of users of DOE open science systems. Human signatures for evaluating and assessing use of systems also need to be developed as part of this PRD. Challenges involve complexities inherent with human factors, the large-scale of traffic, large numbers of users, and distributed, heterogeneous systems. New capabilities will be developed to predict, detect and understand the intention of human attacks, especially "insider" attacks. The research is expected to require five to ten years to achieve fruition, although intermediate aspects may become available in three to five years.
b. **Malware Research Lab (FSA)** – This PRD involves creating an environment to implement and test Cyber Security malware in representative environments. Challenges are the large, complex and evolving instances of malware that must be "mapped onto" a large, complex and evolving set of hardware, software and networks that is often distributed and interacting. New Cyber Security discoveries include novel techniques for copying and duplicating malware, representing systems and environments upon which to "map" the malware, and the ability to assess the effects of malware on these systems so that appropriate protective and countermeasures may be taken. This research area has many similarities to comparative genomics where the Biology metaphor of DNA as the cellular operating system for complex networks of control networks has expressive power. New tools that can rapidly assess and identify a dynamic evolution of open computing systems are needed. The research is expected to require seven to ten years to achieve fruition with advances in computer science, mathematics, computer architecture, large-scale data-intensive parallel computing and visualization.
c. **Security Policy Implementation Impacts on Usability (HF)** – This PRD involves developing a flexible simulation test bed for modeling Cyber Security policies on open science systems, so that they can be tested before being put into production. Metrics and measurements for evaluating and assessing the effectiveness of policies on Cyber Security and usability need to be developed as part of this PRD. Challenges involve complexities inherent with Cyber Security policies in a large-scale, highly distributed environment, the difficulty of translating Cyber Security policy into practice in complex, distributed, heterogeneous environments, and the difficulty in assessing implications of new Cyber

Security policy. New Cyber Security discoveries will eventually include the framework to better understand the impacts of new Cyber Security policy upon systems and users, and more consistent Cyber Security policy and accessibility across multiple, distributed systems. The research is expected to require five to ten years to achieve fruition, although intermediate aspects may become available in three to five years.

d. **Usability of Security (secure) Systems (HF)** – This PRD involves developing new user interfaces to promote the ease and correctness of installation, configuration and maintenance of security systems. In addition, this PRD advocates development of quantitative metrics and measurements for usability. Challenges include the significant complexity inherent in Cyber Security systems and difficulty communicating in this complex environment. New Cyber Security discoveries include the development of metrics and measures to quantify usability of security systems. R&D in this area will provide increased assurance that systems and networks are better protected and result in more efficient and effective Cyber Security operations and greater availability of secure systems, thereby facilitating open science. The research is expected to require five to ten years to achieve fruition.
e. **Improving Cyber Security Practice (SHSD)** – This PRD motivates the development of new trust frameworks and the tools to model, simulate, and analyze trust in open science environments. Risk-benefit analyses for Cyber Security practice must also be developed and exercised. Challenges are that the open science community exists in a highly decentralized environment, involving many sites, each with different policies and infrastructures for trust. New Cyber Security discoveries include novel techniques for trust negotiation among systems and users. It was not determined how long this research might take to achieve fruition.

6. Control Systems

Improving the security of energy control systems is a crucial step for national infrastructure protection. This thrust area provides for research directly into key attributes of control systems: survivability and trustworthiness.

a. **Survivable and Trustworthy Control Systems (UI)** – This PRD involves template architectures for control systems including models of survivability, designs for graceful failure (controlled degradation), and improved support for human intervention. Protection is to be against malicious attacks and accidental failures, accommodate varying reliability requirements, and strike the appropriate balance between safety and performance. Challenges are numerous, including: the distributed, heterogeneous nature of systems and system components, how to quantify, measure and evaluate survivability and trustworthiness with respect to cyber and physical threats, how to identify and prioritize failure and degradation, and the requirement to maintain a high level of service during an incident. New Cyber Security discoveries include the development of comprehensive models of systems that will address holistic factors. Benefits of this PRD are strong and survivable systems, both DOE large-science systems and utility infrastructure. The research is expected to require three to ten years to achieve fruition.
b. **Anomaly Detection in Control Systems (FSA)** – This PRD involves developing a model for system behavior, appropriate parameters for and sensitivity to control systems, and a generic template for anomaly detections for adaptive, self-healing control systems. Challenges are that systems deployed today are more complex than our ability to understand fully, failure modes are not completely predictable, a large diversity (age, high degree of

geographical distribution, and technologies) of systems exist in production, and a wide variety of factors which influence performance including environmental, social, physical network, and the interface between humans and systems. New Cyber Security discoveries include novel techniques for early detection that will be widely applicable to power and control systems. Benefits include greater Cyber Security in control systems, better decision support, and graceful degradation rather than catastrophic failure. The research is expected to require five to seven years to achieve fruition with advancements in computer science, computer architecture, statistics, and the mathematics of complexity.

c. **Electromagnetic Pulse and Cyber Defense (HF)** – This PRD involves analyzing the effects of a catastrophic event such as nuclear detonation at mid to high altitude over the continental United States that could potentially disrupt all electronic systems, including the systems that control our utility infrastructure. Challenges are the scope and breadth of systems that may be affected, and uncertainty in the nature and location of the nuclear device. New Cyber Security discoveries include the development of new materials, methodologies and strategies for shielding and sheltering critical control systems. Additionally, there are social factors, e.g. how to mitigate the effects of such disruption upon society. The research is expected to require three to five years to achieve fruition. There is a clear connection of this PRD to National and Homeland Security.

d. **Understanding Risk and Survivability Assessment (UI)** – This PRD involves developing a comprehensive, real-time, high-performance operational model of control systems, and to evaluate robustness during a security incident. A significant emphasis will on gathering, logging, distilling, anonymizing, and sharing threat data. A security investment model is also a component of this PRD. Challenges are numerous, including: the distributed, heterogeneous nature of systems and system components, how to quantify, measure and evaluate robustness with respect to cyber and physical threats, how to identify and prioritize incident response including factors of cost, how to quantify and predict responses to operator interaction, how to enforce Cyber Security in the face of real-time requirements, and the requirement to maintain a high level of service during an incident. New Cyber Security discoveries include the development of comprehensive models of control systems that will address holistic factors. Benefits of this PRD are trusted and robust systems. The research is expected to require three to ten years to achieve fruition.

7. Future of Cryptography

Current Cyber Security practices depend extensively on cryptography. In DOE's open science environment, it is clear that data sets are becoming too large for today's cryptographic methods. It is also becoming obvious that computing systems will soon become sophisticated enough to easily crack current cryptographic schemes. This thrust area will provide DOE with specific open science research into this topic.

a. **Non-cryptographic Security (HF)** – This PRD involves taking another, completely fresh look at cryptographic security. If malware that impairs or "breaks" mathematical algorithms for cryptography is emergent, virtually all networks and environments become open to packet sniffing. Challenges are the vast scope of the problem – software encryption is embedded throughout our secure systems today and the entrenched and ubiquitous nature of our packet-switched networks. New Cyber Security discoveries include the development of new strategies and methodologies for protecting information, including possible circuit-based

approaches or hardware-based cryptography. The research is expected to require three to five years to achieve fruition.

b. **Trusted Hardware and Crypto Acceleration (SHSD)** – This PRD also involves taking another, completely fresh look at cryptographic technology, for which today's implementations represent a significant bottleneck for performance. As a result, often encryption is not selected for transport, thereby posing a Cyber Security vulnerability. Here, the focus is on developing next-generation cryptographic technologies that can keep up with the demands of the highest speed networks. New Cyber Security discoveries include the development of new algorithms which perform much better, perhaps hardware-based accelerators, and new strategies for secure key exchange. The research is expected to require three to five years to achieve fruition.

NEXT STEPS

The breakout session leaders have identified authors to compose more fulsome descriptions of the PRDs. These will be received by the breakout session leaders, who will edit them for consistency and forward them on to the workshop chairs. The workshop chairs will review the submissions, will edit further for consistency, and consolidate where appropriate. A final report will then be submitted to DOE in sixty- to ninety-days.