## Cybersecurity Assurance

# FY17 YEAR-END PERFORMANCE REPORT[1]

FY17 was a very strong year in the execution and recognition of Berkeley Lab's cyber program. Along with effectively mitigating our risks, Aashish Sharma, a member of our cyber team, was part of a team that was awarded the 2017 Internet Defense Prize, sponsored by USENIX and Facebook (https://internetdefenseprize.org/). Our cyber security program was also successfully assessed/audited by three different external organizations, and we were able to complete our multifactor authentication implementation before DOE's deadline of September 30, 2016.

- **Service and Recognition**: The Internet Defense prize for 2017 was awarded for our research into using Bro to identify and alert on the fundamental characteristics of phishing attacks and is considered a "new approach for detecting credential spearphishing attacks in enterprise settings." The research was a joint collaboration between Berkeley Lab, UC Berkeley, and the International Computer Science Institute, and highlights the benefit of having close ties to the University of California and the research community. Phishing is a top risk facing everyone on the Internet, not just Berkeley Lab and we are very proud of Aashish for winning this prize.

  Berkeley Lab cyber also continued to perform extensive service and outreach to DOE as well as the general community this year. Our staff were actively sought after to speak and inspire the next generation of scientists and cyber analysts and to work with leading cyber researchers to further research into identifying, detecting and combating new cyber risks and threats.

  A new NLCIO Policy Analyst, Rainer Elias, was also hired this year and has led and coordinated policy efforts that affect the Labs and Plants.

- **Audits and Assessments:** The FY17 Financial Statement and FISMA controls audit was conducted during the second half of FY17 and consisted of external and internal network vulnerability assessments and audits of the Financial Management System

[1] This report covers the period from September 2016 to August 2017 since the Annual Performance Report is submitted in late August.

(FMS), the Human Resources Information System (HRIS), and our FISMA controls. There were no findings or observations for Berkeley Lab from this audit.

The triennial Safeguard & Security Review conducted earlier this year included a cyber and information security review of all of Berkeley Lab, including NERSC and ESnet.This is the first time the Safeguard & Security Review did not utilize previous assessments to satisfy the cyber component. No findings were identified, however Cyber Security received a Noted Strength / Best Practice mention during the outbriefing:

> *"LBNL is leveraging the BRO IDS in innovative ways to address cyber security risk beyond the conventional scope of intrusion detection. This had made BRO and its supporting infrastructure important to the overall risk profile.*"

In summary, Berkeley Lab's cyber program had another very strong year, reflecting our continuing commitment to excellent risk-management, broadening engagement with our peers in higher education and DOE, and to achieve a more science-friendly and secure cyber security environment for research.

## RISKS AND MITIGATIONS

Berkeley Lab's overall cyber risk profile primarily remains unchanged. For FY17, the following three risks pose the greatest cyber risk to Berkeley Lab:

1. Targeted Phishing,
2. Ransomware, and
3. Web Servers Vulnerabilities, including SQL injections.

All three of these top risks are not unique to Berkeley Lab and are typical cyber risks for any institution. They also do not necessarily pose a greater risk level when compared with other institutions. To address these risks, Berkeley Lab continues to explore new forms of controls and to share our results with the greater community.

### Targeted Phishing

Targeted phishing is an ongoing cyber security challenge, not only for Berkeley Lab, but for the entire cyber security community. The human factor component of this risk poses an especially unique challenge. Our primary mitigations continue to be user education, detection and preventing privilege escalation. The controls we have in place are continuing to function as anticipated and there continues to be no consequential damage or loss of information.

During FY17, we continued our simulated phishing attacks that we started last fiscal year. 200 staff members enrolled in the program and we completed 4 exercises this fiscal year. Each phishing exercise was modified to make them more difficult to distinguish from real emails,

Individuals can opt-in to receive simulated phishing emails and those who click on the simulated

phishing attachments are redirected to awareness material about phishing.We believe that the phishing exercises have been successful and the feedback that we have received from participants has been positive. We are planning to expand our phishing exercises in FY18.

## Ransomware

Malware that encrypts files, requiring victims to pay a ransom to recover the files, was an emerging risk at the start of FY17, but is now considered one of the top three risks facing Berkeley Lab. This is primarily due to the impact of external perceptions about ransomware and not because of an increase in the risk of ransomware incidents occurring at Berkeley Lab. There have been several high-profile ransomware infections in the media this year and as a result, a ransomware infection at Berkeley Lab could face greater scrutiny or the overall impact of a ransomware incident could be misinterpreted.

The mechanism used to infect computers with ransomware is not new, however ransomware raises some challenging recovery and policy questions, such as what to do if a victim has no backups and there is a desire to pay the ransom to recover the data. Laboratory Sr. Management has been briefed on this potential scenario and the potential need for a policy decision on what to do in this scenario.

To address the risk posed by ransomware, existing malware protections, such as backups, antivirus, email filtering, and email deletion capabilities mitigate the overall risk of a ransomware incident to an acceptable level. During this fiscal year, we have also implemented new Bro policy that can detect ransomware attempting to encrypt files and we have prioritized communication and deployment of new backup solutions and institutional file storage as solutions to recovery. For example, Druva, a cloud based backup service, was deployed this year as Berkeley Lab's enterprise workstation backup service

## Web Server Vulnerabilities including SQL Injection

Attacks caused by web server vulnerabilities continue to pose an ongoing risk to Berkeley Lab. These attacks can occur via SQL injections, where the attacker sends malicious SQL commands to a web server enabling them to view or manipulate data. For example, an attacker could send an SQL command to a web server to expose Personally Identifiable Information.

To address this risk, Berkeley Lab deployed NetSparker Cloud this year to routinely scan our web applications for vulnerabilities. Netsparker Cloud is designed specifically for web servers and applications and complements our current Nessus network vulnerability scanning. It's parallel capabilities enables us to scan all of our web servers and applications in one day, a process that used to take a month.

We also evaluated web application firewall products from several vendors, including CloudFlare, and continue to explore ways to dynamically protect against attacks without requiring coding changes to thousands of unique science web applications whenever a new vulnerability

appears.

Even with these additional tools, vulnerable web servers will always exist on our networks. Some vulnerabilities are not fixable, some web servers may be missed by the scans and, most importantly, existing tools are limited and cannot detect all vulnerabilities. Nevertheless, the overall risk is mitigated to an acceptable level by these tools and our existing cyber controls.

## Emergent Security Risks and Evolving Threats

### Policy and Oversight

The largest single unmitigated risk to Berkeley Lab in the area of cyber security continues to be the risk that compliance-oriented policy will have a negative effect on our cyber program and our core science mission. Funding and expertise for cyber security remain limited resources, so any redirection of those resources reduces the effectiveness of our program.

### Internet of Things

Internet of Things (IoT) devices, such as smart thermostats, light bulbs, door locks, etc. are becoming increasingly popular as the costs have come down. As their popularity grows, so does the potential for these devices to impact cyber risk. Recently, botnets composed of millions of compromised IoT devices have appeared on the Internet. One recent example was the Mirai botnet which caught the attention of mainstream media during the last part of FY16 and early FY17.

While botnets are not a new risk, the size and dynamic nature of IoT botnets such as Mirai have created some operational risk. The primary risk is not that Berkeley Lab hosts will become part of the botnet. Instead, as these huge botnets scan the Internet for new victims, it creates spikes in blocking activity that must be addressed by Cyber Security in real time. The risk is not unique to Berkeley Lab, as other Labs and Plants are also similarly impacted. To help address these spikes, we have recently implemented new blocking technology and are continuing to explore new countermeasures.

### Supervisory Control and Data Acquisition (SCADA) systems

We continue to make progress in mitigating cyber security risk associated with SCADA systems. As our understanding of the use of these systems evolves, we have identified two distinct areas to focus our efforts, operational usage and scientific usage.

In the area of operational usage, we worked with Facilities to prioritize moving SCADA systems to isolated networks, resulting in additional staffing from Facilities to assist in this effort. We have also helped Facilities to mitigate the risk from new purchases of SCADA equipment.

In the area of science, we conducted a preliminary inventory and assessment of SCADA use by scientists and researchers. During the latter part of FY17, we published communication and

guidance to scientists about the risks and precautions they should take when working with SCADA equipment.

## Potential Risk

### Staff Recruitment and Retention

Our philosophy of smart cyber security and detection require very smart people who are willing to work across institutional boundaries and develop new tools to accomplish our ends. These people are hard to find and can be difficult to retain. This past year saw a key cyber analyst leave Berkeley Lab for a local startup company. There also continues to be a shortage of qualified cyber staff, especially in the Bay Area where we face stiff competition from Silicon Valley and other institutions. For example, a vacated cyber security position has been unfilled for 14 months due to a lack of qualified candidates.

# PERFORMANCE: PEMP GOALS, OBJECTIVES AND NOTABLE OUTCOMES

We successfully mitigated the risks as outlined in our annual Risk Assessment / Self Assessment while maintaining a science-friendly environment. We continue to rightsize our controls by tailoring them to the risks that have been identified. Our approach to cybersecurity includes working closely with leading edge researchers and leverages our close ties with the academic community. This approach has been externally assessed multiple times and our work has been recognized by top peers in the cybersecurity community.

In addition to our Significant Outcomes described below, Berkley Lab cyber also continued to participate in DOE enterprise defenses this fiscal year and we also deployed multifactor authentication before DOE's September 30, 2016 deadline.

### DOE Enterprise Defenses

Berkeley Lab's Research and Operations Enclave has the CPP Sensor program installed and participates actively in the cyber federated model. We also have continued to report all reportable incidents to iJC3.

Berkeley Lab has indicated its willingness to participate in the DEX program but this program remains on hold as it transitions to E3A. As a new activity this fiscal year, we began working towards installation of an ODIN sensor on the Lab network.

### Multifactor Authentication

Early this FY, Berkeley Lab completed implementation of its Multifactor Authentication Implementation Plan, meeting the DOE deadline for multifactor authentication implementation and achieving 100% compliance for Privileged and Standard Users.

Our approach to multifactor authentication meets the NIST 800-63-2 Level of Assurance

requirements for Privileged and Standard Users and:

- is more suitable for an open science environment,
- is better integrated with our existing cyber program, and
- provides us with the flexibility to adapt to the changing cyber and risk environment.

Our MFA implementation was assessed by Internal Audit Services early this FY as part of two advisory efforts. The first advisory effort focused on evaluating our implementation plan against DOE MFA and NIST 800-63-2 Level of Assurance requirements. The second advisory focused on evaluating our actual implementation. No findings or concerns about our MFA implementation were identified in either advisory effort.

# SIGNIFICANT ACCOMPLISHMENTS

## Communication and Outreach

The Internet Defense Prize, won by Aashish Sharma, is a significant accomplishment, not only for Aashish, but also for Berkeley Lab's cyber program. It recognizes Berkeley Lab's leading edge efforts to work with top researchers to develop and test new countermeasures to risks directly facing the Lab. Phishing is one of our top risks, and Aashish's work is currently being used in production at Berkeley Lab to address this risk. This work also has the potential to benefit other Labs and Plants.

Berkeley Lab's cyber team also continued to provide support to other Laboratory and University sites using Bro, through presentations conferences, and 1:1 consulting with other cyber security teams. We also continue to seek out opportunities to consult with private industry about our cyber program and Bro this year.

In FY17, Berkeley Lab cyber discussed Bro and our cyber approach with:

- Tanium
- Marist College
- Jet Propulsion Laboratory
- John Hopkins University
- California Institute of Technology
- Visa, Inc.
- SLAC
- University of Michigan
- Netflix

As part of our outreach to the broader community, especially to showcase Berkeley Lab's diversity in cyber, Berkeley Lab cyber participated in the following community events this fiscal year:

- Albany High School career day

- Burton High School girls talk
- SULI,BLUR,CCI interns Cybersecurity talk September 2016 and January 2017
- Women in Technology Symposium: Recognizing leaders, inspiring the next generation
- America's Summit: Women Entrepreneurs Day @ Facebook
- TECPUI interview
- Women Economic Empowerment for UN March 29th 2017
- Cyber Workforce Development Exploratory Meeting @Argonne National Laboratory March 31th - April 1st 2017
- Cyber security talk for Kennedy High School
- Keynote for cybersecurity and gender conference Cybersecurity Work and Research - Lawrence Berkeley National Laboratory
- Speaker at the 3rd Annual SF International Women Entrepreneurs Forum Gran Canaria Summit 2017: The challenge of Cybersecurity

In support of DOE's iJC3 effort, Berkeley Lab continues to lead the iJC3 Cyber R&D group and to be a partner in the iJC3 Data Fusion group. The Berkeley Lab iJC3 Cyber R&D effort is being led by Dr. Sean Peisert, however Berkeley Lab cyber will be lending its operational expertise with Bro and data fusion as part of the effort. Unfortunately, DOE's iJC3 effort this fiscal year focused on defining the operational scope and direction for iJC3, and they have placed Cyber R&D at a very low priority.

Berkeley Lab has also continued our ongoing collaboration this fiscal year with the larger UC system, sharing our knowledge and expertise with our counterparts at other UC locations. The Berkeley Lab CIO was part of a leadership team at UC that was structuring future security improvements for the entire UC system and our CISO participated in UC cyber security activities.

### Service

Berkeley Lab CIO continues to play a significant role in National Laboratory CIO efforts to represent the interest of the National Labs at the Federal level. The Berkeley Lab CIO is part of the executive committee of the NLCIO and has led efforts to educate new administration officials through multi-lab reverse site visits to DOE Headquarters. In addition to this leadership role, Berkeley Lab continues to dedicate resources to outreach and best-practice sharing with peer laboratories and research universities, as well as private sector companies, to improve cyber security on the internet.

## INTEGRATED ASSESSMENTS

| Assessment Area | Assessment Description | Assessor | Quarter Due | Status of Assessment |
|---|---|---|---|---|
| IT | Safeguard and Security Review | SC | FY17Q1 | Report Issued |
| IT | OMB Circular A-123 - IT Controls | IAS | FY17Q2 | Report Issued |

| | | | | |
|---|---|---|---|---|
| IT | Financial Systems / FISMA Controls Audit | KPMG / OIG | FY17Q3 | Report Pending |
| IT | Quarterly Review of Cyber Controls | IT | Ongoing | Ongoing |
| IT | Risk Assessment Self Assessment | IT | FY17Q1 | Report Issued |
| IT | Multifactor Authentication Implementation (Advisory) | IAS | FY17Q1 | Report Issued |
| IT | NIST Cybersecurity Framework Assessment | UC | FY17Q2 | Report Issued |

### FY17 Financial System / FISMA Controls Audit

Berkeley Lab was selected this FY by OIG for a Financial System (FISCAM) and FISMA controls audit starting in FY17 Q3. The last time that Berkeley Lab had a FISMA controls audit was in 2012. This year's audit required a substantial amount of effort from the cyber security program during FY17 Q2 and FY17 Q3, especially since it included internal and external network vulnerability assessments. The final report is expected to be issued FY18 Q1 and we do not expect any findings or observations.

### Office of Science Safeguard & Security Review

In addition to the FISCAM / FISMA controls audit, an assessment of Berkeley Lab's information and cyber security was conducted in late January / early February as part of a triennial Office of Science Safeguard & Security Review. The review included a comprehensive assessment of cyber and information security controls for all Berkeley Lab's enclaves (ROE, BSE, ESnet and NERSC). There were no findings for information security or cyber security, and cyber received the only "Noted Strengths / Best Practices",

> *"LBNL is leveraging the BRO IDS in innovative ways to address cyber security risk beyond the conventional scope of intrusion detection. This had made BRO and its supporting infrastructure important to the overall risk profile.*"

### University of California NIST Cyber Security Framework Assessment

Berkeley Lab's cyber program was also assessed by the University of California as part of a system-wide NIST Cybersecurity Framework assessment during FY17 Q2. Our existing NIST 800-53 control families were mapped to the NIST Cyberecurity Framework and were assessed by UC Internal Audit and UC Cyber Risk Management. The final report was issued in FY17 Q3 and there were no findings or observations noted.

### Multifactor Authentication Assessment

At the end of FY16, Berkeley Lab CIO requested that Berkeley Lab Internal Audit Services perform an advisory assessment of Berkeley Lab's Multifactor Authentication Implementation Plan. The goal of this advisory assessment was to provide a third party review of Berkeley Lab's MFA implementation and to validate meeting NIST 800-63-2 Level of Assurance requirements

for Privileged Users and Standard Users as defined in the June 26, 2016 version of the DOE Multifactor Authentication Implementation Approach document.

The advisory assessment was conducted in two parts, the first part focused on Berkeley Lab's implementation plan and if it met DOE MFA and the NIST 800-63-2 Level of Assurance requirements. The second part focused on the actual MFA implementation. The final report was issued at the end of January 2017. No deficiencies were identified.