TRUSTED CI
THE NSF CYBERSECURITY
CENTER OF EXCELLENCE

2017 NSF Community Cybersecurity Benchmarking Survey Report

8 June 2018
For Public Distribution

Scott Russell,[1] Craig Jackson,[2] Bob Cowles

[1] Project Lead, scolruss@indiana.edu
[2] NSF CCoE Co-PI, scjackso@indiana.edu

About the NSF Cybersecurity Center of Excellence

Our mission is to provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.

Acknowledgments

The authors thank Jim Marsteller and the members of the Trusted CI team who participated in the development and socialization of the survey, and to all other team and community members who contributed ideas regarding the content of the survey. Special thanks go to Kay Avila for her help in reviewing and refining the analysis.

Many thanks to all the respondents.

This document is a product of Trusted CI. Trusted CI is supported by the National Science Foundation under Grants Number ACI-1547272. For more information about the Trusted CI please visit: https://trustedci.org/. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

Using & Citing this Work

This work is available on the web at the following URL:
http://hdl.handle.net/2022/22171

Table of Contents

Executive Summary **4**

1 Introduction **5**

2 Methodology **5**

2.1 Responding Community and Audience 5

2.1.1 NSF Project Community 5

2.1.2 Audience for This Report 5

2.2 Survey Construction 6

2.3 Response Collection 6

2.4 Response Evaluation 6

3 Results **6**

3.1 Response Rates 7

3.2 Response Categorization 7

4 Analysis **7**

4.1 Project or Facility Budget 7

4.2 Project or Facility Attributes 8

4.3 Cybersecurity Programs and Practices 9

4.4 Cybersecurity Concerns 11

5 Conclusion **12**

Appendix A: Survey **13**

Instructions for completing survey 13

Project or Facility Budget 13

Project or Facility Attributes 13

Cybersecurity Program 14

Cybersecurity Concerns 17

Feedback 18

Appendix B: Tables of Survey Results **19**

Project or Facility Budget 19

Project or Facility Attributes 20

Cybersecurity Program 22

Cybersecurity Concerns 27

Executive Summary

The purpose of this survey is to collect, analyze, and publish useful baseline benchmarking information about the NSF science community's cybersecurity programs, practices, challenges, and concerns. We received 20 responses to this year's survey, including 18 from respondents with annual budgets greater than $1M, and 15 from NSF Large Facilities. The mean total budget of respondents was $45,380,000, and the median budget was $45,000,000. This was the second year of the NSF Community Cybersecurity Benchmarking Survey. Highlights from the results and findings include the following:

A. Respondents' cybersecurity budgets vary widely, with Large Facilities having budgets ranging from 0.005% to 4% of annual budget for those with a non-zero budget (a wider range than 2016's 0.02% - 1.5% annual budget). This variability increases when controlled for IT budget.
B. 4 of the 15 Large Facility respondents cannot provide a discrete cybersecurity budget.
C. Respondents do not agree on what costs are included in their cybersecurity budget, with labor, software, and hardware all left out by a subset of respondents. Greater standardization on what comprises a cybersecurity budget would be a valuable step toward understanding cybersecurity in the science community.
D. Respondents inconsistently establish cybersecurity officers (e.g. CISOs) with 4 respondents (including 3 Large Facilities) having no cybersecurity officer, and 12 respondents having a cybersecurity officer operate only part-time. Only 4 respondents have a full-time cybersecurity officer. These findings do not correlate with differences in annual, IT, or cybersecurity budgets.
E. The large majority of respondents authenticate users from multiple institutions, with 14 authenticating from more than 3 external sites, and 17 authenticating from at least 2.
F. There is a great deal of variability in how respondents implement key elements of their cybersecurity programs, with operational safeguards, programmatic safeguards, software development practices, cybersecurity framework selection, and residual risk acceptance all varying widely between organizations. This variability appears to be unrelated to organizational size or budget. The great deal of variability in these findings suggests that cybersecurity governance is not consistently practiced across facilities.
G. Multi-factor authentication is adopted by 12 of the 20 respondents (60%), a notable increase from 2016, which had only 6 positive respondents out of 27 (~22%).
H. Residual risk acceptance is inconsistently practiced, and there is a lack of consistency among those who do practice it, suggesting that more training on this would prove valuable to the community.
I. The majority of respondents are required to comply with external cybersecurity requirements, with the most common requirement being the terms of their NSF Cooperative Agreement (14).
J. 18 of 20 respondents develop software in-house. This is in accord with the 2016 Survey, in which all of the respondents said they develop software in-house.
K. Patching times are highly variable, with critical patches ranging from 2 days up to a month to implement. Furthermore, many respondents treat sub-critical patches categorically similarly, with important, moderate, and low often dealt with on similar timescales. This suggests that respondents may have difficulty understanding and acting upon the relative importance of non-critical patches.
L. Respondent's known incidents do not directly track with total budget, IT budget, or cybersecurity budget. 8 of the 20 respondents claim either "None" (6) or "Don't Know" (2) for incidents, which may suggest problems with incident detection.
M. Respondents say their greatest concern regarding cybersecurity is from loss of availability or malicious manipulation of data, suggesting a notable focus in the NSF science community on integrity and availability in the Confidentiality, Integrity, Availability (CIA) triad.

1 Introduction

Benchmarking information is frequently used to develop a common sense of status and norms within a community or sector. At the 2015 NSF Cybersecurity Summit, the audience indicated that there was interest in generating a survey of the state of cybersecurity for the NSF science community, and that the community would respond to the survey and utilize the results. Based on this positive feedback, Trusted CI set out to conduct its first annual community survey in 2016, releasing the report from the first year's results on April 28, 2017. The first report was well received, and the second report initiated.

The purpose of Trusted CI's Community Survey project is to collect, analyze, and publish useful baseline benchmarking information about the NSF science community's cybersecurity programs, practices, challenges, and concerns.

The remainder of this report is as follows: Section 2 describes the methodology for constructing the survey and collecting responses; Section 3 presents an overview of the survey data collected; Section 4 provides analysis of the survey data; and Section 5 concludes with broader reflections and next steps.

2 Methodology

In this section, we describe our target respondent community, target audience for this report, survey construction, and response collection.

2.1 Responding Community and Audience

2.1.1 NSF Project Community

NSF awards approximately 27% of the total federal budget for basic research, supporting over 350,000 researchers, post-doctoral fellows, trainees, teachers, and students.[3] Among the NSF's active awards are ~25 NSF Large Facilities (LF).[4] This survey was targeted to the NSF community of science projects and facilities.

2.1.2 Audience for This Report

We envision three primary audiences for this report:

- NSF-funded science projects and facilities. The survey results may assist large science projects and facilities in developing a sense of norms and practices in the community.
- NSF leadership and program officers. The survey results may give NSF leadership and program officers greater insight into norms and practices in the community.
- Trusted CI. The survey results will assist Trusted CI in tailoring its services to the current

[3] https://www.nsf.gov/news/news_summ.jsp?cntn_id=100595

[4] https://www.nsf.gov/bfa/lfo/docs/large-facilities-list.pdf

state of cybersecurity at NSF-funded projects and facilities.

2.2 Survey Construction

We designed survey questions to collect information on respondents' budgets and other descriptive attributes relevant to cybersecurity, including information on specific cybersecurity practices, events, and concerns. The survey was updated after the 2016 Community Survey Report to provide greater insight into cybersecurity practices of the respondents. On August 8, 2017, we made the survey available for Trusted CI's review. A text copy of the survey is included as Appendix A.

Response to this survey was voluntary and optional. To encourage a higher response rate and more complete responses, we purposely avoided collecting project identifying information (e.g., project name, award number).

2.3 Response Collection

The survey was announced on August 14, 2017 on Trusted CI's Blog.

At the NSF Cybersecurity Summit on August 16, 2017, Von Welch highlighted the survey during his talk on Trusted CI. The survey was explicitly mentioned at the Large Facility Security Team meetings during the months of August, September, and October. Reminders were posted to the Trusted CI Announce email list on October 18, November 2, and November 13. The response period for responding to the survey closed on November 17.

2.4 Response Evaluation

Responses were evaluated at face value, despite some responses falling far outside of expected ranges. Averages were calculated based solely on non-null/non-zero responses in calculating average; including null/zero responses in the budget averages would have skewed the results and led to misleading averages.

The responses were compiled in a spreadsheet, with questions broken down to represent each possible answer when multiple answers were allowed, and with additional space for calculated answers, such as the respondent's cybersecurity budget as a percentage of IT budget. This spreadsheet was utilized to develop a preliminary analysis of the results, culminating in the development of a Preliminary Findings document that was circulated on the Trusted CI team listserv on March 9, 2018.

3 Results

Below, we provide a high level picture of the response rates and the categories of respondents that emerged in this response group.[5]

[5] See Appendix B for tables detailing the results from the survey. Note that some questions were not answered by all

3.1 Response Rates

The survey received 20 responses. In light of the thousands of active NSF awards, we caution against any conclusion that these results are representative of the community at large. However, we received responses from 15 of the ~25 Large Facilities, plus 3 additional responses from awards with annual budgets greater than $1,000,000.

3.2 Response Categorization

Using the methodology set out from the 2016 survey, we continued to group the respondents by annual budget, with the three categories consisting of: 1. **Large Facilities** (15) - a specific designation by NSF; 2. **Big** (3) - respondents with annual budgets over $1M; and 3. **Small** (1) - respondents with annual budgets under $1M. Considering the high relative response rate of large facilities on this year's survey (15 out of the 20 respondents), our analysis is primarily related to the cybersecurity of Large Facilities, but does include discussion of the other 5, non-LF respondents.

4 Analysis

In this section, we provide high level analysis of the survey responses, highlighting results that were particularly interesting, unexpected, notable, or concerning. Considering the majority of respondents were Large Facilities, our analysis is largely focused on the security implications for Large Facilities. The relevant survey question is denoted with a letter-number pair in square brackets (e.g., [Q6]) (for the full question text, see Appendix A).

4.1 Project or Facility Budget

Respondents were asked to provide the annual budget [Q1], the annual IT budget [Q2], and the annual cybersecurity budget [Q3] for their project or facility. Annual budgets among the Large Facilities ranged from $8M to $100M, and overall the mean budget was $45.38M and the median budget was $40M. Even considering this range of annual budgets, cybersecurity budgets among the respondents varied wildly, with some Large Facilities listing explicitly $0, others as low as $2000. On the top end, one Large Facility said it budgets as much as $2M for cybersecurity. When controlled for both annual and IT budget, this variability only increased, as the increasing cybersecurity budgets did not appear to correspond with increasing annual or IT budgets. Indeed the range of cybersecurity as a percentage of IT budget is perplexing, with Large Facilities ranging from .02% up to 20% (excluding budgets of $0), and one non-Large Facility at 26.5%.[6] Additionally, 4 Large

respondents; some questions allowed multiple selections as a response; and some questions allowed no more than two selections.

[6] Note that this range lies outside both extremes seen in industry, where the highest subgroup (small finance companies) topped out at ~14% of IT budget, and the lowest at ~2% of IT budget. *See, e.g.,* Scott Russell, Craig Jackson, Robert Cowles, Cybersecurity Budgeting: A Survey of Benchmarking Research and Recommendations to Organizations, presented at and published in the report of the 2016 NSF Cybersecurity Summit, Arlington, VA, 17 Aug 2016.

Facilities could not specifically calculate their cybersecurity budgets.[7]

One potential explanation for this variability is that what organizations included in their cybersecurity budgets is not consistent across organizations. Some organizations opt to not include one or more of labor (4), hardware (4), and software (6) [Q4], while 5 respondents marked “Other,” although they did not specify what these other costs included. Adding to the complexity, identifying when labor, hardware, or software qualify as “cybersecurity” costs is not always clear, as a number of cybersecurity best practices are also simply good IT practices, such as applying patches or practicing code hygiene. Greater standardization in this regard would be valuable to improve the study of cybersecurity budgets within the science community.

	LF category	Overall
Cybersecurity as % of Annual Budget (mean value)	0.731%	1.06%
Cybersecurity as % of Annual Budget (non-zero range)	0.005% - 4%	0.005% - 4%
Cybersecurity as % of IT Budget (mean value)	6.15%	6.86%
Cybersecurity as % of IT Budget (non-zero range)	.2% - 20%	0.2% -26.47%

Other potential explanations for the variation in cybersecurity budgets include, but are not limited to: (a) budget sizes are largely driven by facility or project mission or needs assessment rather than adhering to some budgetary rule of thumb; (b) respondent leadership beliefs regarding the need for cybersecurity investment vary greatly; (c) a lack of understanding as to appropriate methodologies for crafting budgets and evaluating risks, or (d) respondent error. For the non-Large Facility respondents, this variability is more to be expected, as particularly small awards may rely entirely on a parent organization for their cybersecurity needs, whereas mid-sized awards may vary greatly based on their reliance on IT infrastructure.

4.2 Project or Facility Attributes

Survey questions in this group were meant to uncover information about the environment in which cybersecurity takes places.

4.2.1 Nearly all respondents had complex authentication environments, with 17 of 20 accommodating users from multiple external institutions [Q6] and 14 indicating a need to

[7] The 4 Large Facilities that did not provide a cybersecurity budget stated: “Included in overall IT budget,” “No separate budget for cybersecurity,” “Not centralized,” and “Difficult to estimate.” (Some details have been omitted to preserve respondents’ anonymity.)

authenticate from more than three external institutions. These responses were largely irrespective of annual budget, with 3 non-Large Facilities authenticating from more than three external locations, and one Large Facility not authenticating from any external locations.

4.2.2 The role of cybersecurity officer, such as a CISO, ISO, or CSO, varied greatly among the respondents as well. Although a majority of respondents had a cybersecurity officer (16 of 20), the clear majority operated only "part-time" (12 of 16), with only 4 respondents employing full-time cybersecurity officers. The practice of employing a cybersecurity officer did not seem to track with annual budget, IT budget, or cybersecurity budget. One respondent employed a full-time cybersecurity officer without being able to identify a cybersecurity budget, and another with a budget of only $2000. Yet on the other extreme, two facilities with annual budgets over $70M employed no cybersecurity officer, and three organizations with cybersecurity budgets at or over 20% of IT budget only employed an officer part-time. This disparity between budgetary practices and cybersecurity leadership is hard to reconcile, and indicates that cybersecurity governance is not consistently practiced across facilities.

4.2.3 Cybersecurity Full Time Employees (FTEs) [Q8] roughly tracked with cybersecurity budgets, excepting those respondents who did not include labor in their budget calculations [Q4]. Notably, almost half of all respondents (9/20) employ the equivalent of 1 cyber FTE or less.

4.2.4 Software best practices were variably implemented across respondents. 18 out of 20 respondents developed or maintained software in house [Q9]. Of those who did, 15 used interpreted languages, and 14 used compiled languages. Bug Management (17) and Code Repositories (15) were the most widely practiced, with near universal adoption, whereas Static and Dynamic Analysis (1) and Code Signing (4) were almost never adopted. It is unclear whether there is a legitimate reason for these disparate results, or if the particular practices implemented are simply a product of ease and/or familiarity. Indeed, initial circulation of these findings within Trusted CI prompted feedback that the extremely low use-rate of Static and Dynamic Analysis in particular was troubling, suggesting that NSF facilities could benefit from educational materials to encourage adoption of more of the secure software development practices.

4.3 Cybersecurity Programs and Practices

4.3.1 The majority of respondents engage in some policy development (16 of 20) [Q10]. The most widely used role for policy development was an IT or cyber manager (13 of 16). However, a number of facilities or projects identified multiple organizational elements that participate in policy development, with 8 using and 2 considering a Governance Board, 4 using their Principal Investigator, and 10 relying to some degree on the processes of their parent institution. Interestingly, 3 of the 4 respondents who identified having "no process" also identified organizational roles in charge of policy development, suggesting that despite formalized responsibility for policy development, there was no formal policy adoption process.

4.3.2 Almost all of the respondents utilized some form of framework or guidance (19 of 20) [Q11]. The most popular frameworks were the Trusted CI Guide (10 of 20), NIST Risk Management Framework (10 of 20), and CIS Controls (9 of 20). The Australian Signals Directorate's Essential 8, ISO 27005, and Interoperable Global Trust Federation each netted zero respondents.

4.3.3 Residual risk acceptance was inconsistently implemented [Q12], with nearly half of the respondents selecting "There is no explicit risk acceptance process" (9 of 20), of which 5 were Large Facilities. Among those with residual risk acceptance processes, the role of risk acceptor varied greatly, with "IT manager" as the most common (6), while the remainder were roughly equally distributed between "a cybersecurity person" (2), "system or process owner" (2), "senior managers or PI" (3), and "an individual in the parent institution" (3). This sparse and inconsistent practice suggests that guidance on residual risk acceptance would prove valuable to the community.

4.3.4 The majority of respondents are subject to external cybersecurity requirements (15 of 20) [Q13], with the terms of their cooperative agreement being the most common (14 of 20).[8] Personally Identifiable Information (8), Protected Health Information (6), and Non-Disclosure/Contractual Agreements (9) were also fairly common. No respondents selected "Don't Know," suggesting widespread perceived awareness of external cybersecurity requirements.

4.3.5 A subset of programmatic safeguards enjoy widespread adoption [Q15], with 15 respondents implementing an overarching cybersecurity strategy, 15 adopting a specific incident response policy, 13 having documented cybersecurity standards, 12 utilizing a business continuity plan, 12 adopting roadmaps to implement cybersecurity improvements, and 12 utilizing an inventory. Maturity models (3), data classification schemes (7) and external reviews (5) were the least commonly practiced.

4.3.6 A subset of operational safeguards [Q16] are widely adopted, such as central logging (14), vulnerability scanning (16), firewalls (16), and anti-virus (16). Practices with low adoption rates are penetration testing (4), tabletop exercises (4), and data loss prevention and encryption (8). It is unclear why such large discrepancies exist between individual controls, raising the possibility that more training and awareness could increase the adoption rate of operational safeguards.

4.3.7 Multi-factor authentication (MFA) is adopted by 12 of the 20 respondents (60%), a notable increase from 2016, in which only 6 of 27 (22%) respondents utilized MFA. Although a notable improvement, the importance of MFA is so pronounced that it is still troubling to see that 40% of respondents, including 7 Large Facilities, are not utilizing it. Further inquiry may be needed to identify any specific problems that are preventing community members from taking advantage of this control.

[8] Note, that all Large Facilities are subject to cooperative agreement terms, so at least one Large Facility is not aware of the cybersecurity requirements listed in their CA. Additionally, two respondents identified both "none" and "cooperative agreement terms from NSF," suggesting some potential confusion.

4.3.8 Patching times vary greatly between respondents, and even within respondents depending on the criticality of the patch [Q17]. For critical patches, respondents' response times range from 2 days to 1 month to implement, with the most common answer being 1 week (9 of 20). Outside of critical patches, response times vary more greatly, with important patches ranging from 2 days to 3 months, and moderate and low importance patches ranging from 1 week to greater than 3 months. Of particular note is an apparent trend of organizations to treat all non-critical patches at roughly the same timescale. For instance, one respondent dealt with "critical" patches within 2 days, but "important," "moderate," and "low" patches all required 3 months. While this is an extreme example, a number of respondents treated non-critical patches identically, suggesting respondents have difficulty determining how to manage sub-critical risks. One possible explanation for this collapse of risk categories is that "critical" patches may receive special attention, and all others are simply addressed during the next routine patch, regardless of relative importance.

4.3.9 12 out of 20 respondents detected at least one incident in the past year, with 5 detecting more than 3 [Q18]. The remaining 8 out of 20 respondents selected either "None" (6) or "Don't Know" (2). Tracking of incidents appears to be unrelated to organizational budget, IT budget, or cybersecurity budget. It is important to note that this only represents "detected" incidents, as organizations cannot list breaches or other adverse events that they did not detect.

4.3.10 Of the respondents who listed at least one cybersecurity incident, the most commonly cited concerns arising from those incidents are the cost of remediation (5) and the inability to analyze data (5) [Q19].

4.4 Cybersecurity Concerns

4.4.1 Respondents cite "workstation compromises" as having the largest operational impact (9 of 20) [Q20], whereas none of the respondents list portable devices or data theft/alteration as their primary concern.

4.4.2 Respondents cite "larger cybersecurity budgets" as the improvement that would most strongly benefit cybersecurity. Note, this includes respondents with the highest existing budgets, but did not include any organizations that could not provide a specific cybersecurity budget. This may suggest that separately delineating cybersecurity budgets helps organizations to better identify when those budgets are inadequate. (Conversely, this may also mean that not delineating budgets makes it more difficult to identify when those budgets are inadequate.) However, the question's focus on "budgets" rather than resources more broadly may have precluded organizations without a formalized budget from selecting this response.[9]

4.4.3 Respondents list "loss of availability" as their biggest concern regarding an incident (12) [Q22], with unauthorized modification (7) and unauthorized access (8) following. This highlights the

[9] This question will be updated in subsequent Community Surveys to address this potential point of confusion.

pronounced focus on integrity and availability in the NSF science community.

5 Conclusion

This year's survey saw a dramatic increase in response-rate from NSF Large Facilities, providing valuable insight into the security programs, practices, and concerns of this unique community. We hope that these results and the subsequent analysis provide some benchmarking insight and inspire discussion, particularly for Large Facilities and projects with larger budgets. Looking ahead, Trusted CI will use this report and past community survey reports to fuel discussions and inform its services. Moreover, we will look for community feedback on changes to future surveys to improve its salience to the community.

Although we received too few responses to claim a representative sample of the NSF science community as a whole, the high response rate of Large Facilities provides greater insight this subset of NSF facilities, and the overall dataset should still offer interesting (and sometimes concerning) insights into the state of cybersecurity in the NSF science community. Future surveys will explore options for increasing the response rate of smaller projects, such as the use of an abbreviated survey that smaller projects could more easily respond to.

Now having administered the survey for a second year, we have identified additional areas for improvement:

- Questions regarding incidents should be clarified as to their scope, and concerns arising from incidents should include hypotheticals to ensure that the priorities of respondents who didn't detect incidents are still captured.
- Questions regarding practices could include an option for respondents to identify controls or other practices that they do not currently implement, but would like to. Similarly, these questions could allow respondents to rate how they would prioritize practices they do not currently implement.
- Questions with options that generalize responses over a certain number (e.g. >3 incidents) should allow a space for respondents to enter the specific number.
- Questions clarifying how respondents use certain high-value controls, such as multi-factor authentication (e.g., whether they are required for all, or only some subset of accounts and accesses).
- The NIST Cybersecurity Framework (CSF) should be included in the list of potential frameworks for respondents to select from.
- We will be looking to the community to determine if an abbreviated survey may prove more useful on an annual basis, with more in-depth surveys being conducted at two year intervals.

Appendix A: Survey

NSF Community Cybersecurity Benchmarking Survey

Instructions for completing survey

An NSF project or facility should submit only a single response to this survey. Completing the survey may require input from from the PI, the IT manager, and/or the person responsible for cybersecurity (if those separate areas of responsibility exist). While answering specific questions is optional, we strongly encourage you to take the time to respond as completely and accurately as possible. If you prefer not to respond or are unable to answer a question for some reason, we ask that you make that explicit (e.g., by using "other:" inputs) and provide your reason. CTSC will release results that we believe provide anonymity to the individual project or facility respondents.

Project or Facility Budget

If you are unable to answer, please provide a reason in the space provided

1. What is your project or facility's annual budget?

Estimate to 1 or 2 significant digits, e.g., $3M, $500K, $23,000

2. What is your project or facility's annual information technology budget?

Estimate to 1 or 2 significant digits, e.g., $1M, $50K, $23,000

3. What is your project or facility's annual cybersecurity budget?

Estimate to 1 or 2 significant digits, e.g., $0.1M, $50K, $23,000

4. What expenses are included in the cybersecurity budget?

Check all that apply

- Labor
- Hardware devices (e.g. firewalls, scanner, forensic devices)
- Software licenses
- Not Applicable
- Don't Know
- Other

Project or Facility Attributes

5. Is your project or facility an NSF Large Facility?

List of Large Facilities -- https://www.nsf.gov/bfa/lfo/docs/LargeFacilitiesListFeb2016.pdf

- Yes
- No
- Don't know

6. Do individuals from multiple institutions authenticate to the resources of your project or facility?

- Yes - 2 or 3 institutions
- Yes - more than 3 institutions
- No
- Don't know

7. Does your project or facility have a person with defined authority for developing and maintaining a cybersecurity program (e.g., ISO, CSO, CISO)?

- Yes, full-time
- Yes, part-time
- No
- Don't know

8. Approximately how many FTEs are involved with cybersecurity work (programmatic or operational) within your project or facility?

- None
- More than 0 up to .5 FTE
- 0.5 to nearly 1.0 FTE
- 1 to nearly 2 FTE
- 2 to nearly 3 FTE
- 3 to nearly 4 FTE
- 4 FTE or greater
- Don’t Know
- Other

9. Does your project or facility develop or maintain software? If so, what policies, processes or tools do you use?

Check all that apply

- Coding standards
- Interpreted languages (e.g., PHP, Python, Ruby, Perl)
- Compiled languages (e.g., C, C++, Rust, Java)
- Source code repositories
- Automated testing
- Continuous Integration
- Static and/or dynamic analysis
- Issue tracking / vulnerability management
- Testing policy (e.g., regression testing of patches)
- Code signing
- Automated documentation tools (e.g., pydoc)
- Not applicable
- Other

Cybersecurity Program

10. How are cybersecurity policies developed and officially adopted within your project or facility?

Check all that apply

- IT Manager or cybersecurity person is responsible
- A formal governance board or group has been established to authorize the policies
- PI or other project or facility leadership are responsible
- There is no formal authorization or adoption process
- The host institution(s) provide the policies
- Other

11. What framework or guidance (if any) has your project or facility adopted for how cybersecurity is done?

Check all that apply

- CIS Critical Security Controls (a. k. a. SANS Top 20) - https://www.sans.org/critical-security- controls
- Australian Signals Directorate (ASD) Top 4/Essential 8
- NIST Risk Management Framework - http://csrc.nist.gov/groups/SMA/fisma/framework.html

- ISO (ISO/IEC 27005)
- Interoperable Global Trust Federation (IGTF)
- CTSC's Guide - http://trustedci.org/guide/
- The parent institution is responsible for the framework
- None
- Other

12. Who accepts residual cybersecurity risk (i.e., the remaining risk after reasonable cybersecurity controls are established)?

Check all that apply

- A cybersecurity person
- IT manager
- System or process owner
- Senior managers or PI
- An individual in the parent institution (external to the project)
- There is no explicit risk acceptance process
- Don't Know
- Other

13. What external cybersecurity requirements (if any) are imposed on your project or facility?

Check all that apply

- State or federally protected Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Non-disclosure or contractual agreements (NDA)
- Classified information - https://en.wikipedia.org/wiki/Classified_information_in_the_United_States
- FISMA / NIST RMF
- CUI / NIST SP 800-171
- Cooperative agreement terms from NSF
- None
- Don't know
- Other

14. What kind(s) of identity management does your project or facility employ to control access to its resources?

Check all that apply

- The parent institution's identity management
- Separately maintained project or facility userid/password
- Independent project or facility certificate-based infrastructure
- Federated identity management technology
- Other

15. What programmatic cybersecurity safeguards has your project or facility implemented?

Check all that apply

- Utilize cybersecurity maturity model to assess and/or plan program evolution
- Have an overarching cybersecurity strategy, policy or plan
- Have a roadmap for cybersecurity improvements
- Have documented cybersecurity standards/baselines for employees and/or external researchers
- Inventory critical information assets
- Have a data classification scheme
- Have a cyber incident response plan

- Have business continuity/disaster recovery plans
- Require periodic cybersecurity awareness training for personnel
- Conduct risk assessments
- Monitor/analyze security intelligence
- Have an Information Security governance structure
- Review by external organizations
- Utilize programmatic safeguards of parent institution
- None
- Other

16. What operational cybersecurity safeguards has your project or facility implemented?

Check all that apply

- Multi-Factor Authentication
- Centralized logging system
- Vulnerability management
- Scan for vulnerabilities or configuration errors
- Physical access controls to critical resources
- Intrusion Detection Systems / IPS
- Network firewalls that block all but required access ports / protocols
- Anti-virus / Anti-spam / spyware / phishing solutions
- Data loss prevention / file encryption
- Real-time alerting of possible attacks / anomalies
- Internal tabletop exercises to gauge organizational response
- Penetration or phishing tests
- Utilize operational safeguards of parent institution
- None
- Other

17. How frequently are patches applied based on the severity rating, either on a fixed maintenance cycle (e.g., monthly) or based on some regular cycle after a patch is released?

Choose a single value for each row. If multiple values are appropriate depending on system type, choose the shortest interval.

	2 Days	1 Week	1 Month	3 Months	> 3 Months
Critical					
Important					
Moderate					
Low					

18. How many cybersecurity incidents (i.e., any event that puts the confidentiality, integrity, or availability of data or information systems at risk) has your project or facility experienced in the past year?

- 1
- 2
- 3
- >3
- None
- Don't know

- Prefer not to answer

19. For the cybersecurity incidents your project or facility experienced in the past year, what were the programmatic impacts?

Check all that apply

- Loss of reputation
- Decreased confidence in data integrity
- Temporary or permanent inability to collect or analyze data
- Interruption of remote access
- Sanctions or legal actions due to breach of sensitive information
- Significant cost of incident recovery procedures
- Cost of additional remediation procedures / controls
- Does not apply
- Other

20. For the cybersecurity incidents your project or facility experienced in the past year, which have had the greatest operational impact?

Check no more than 2

- Network denial of service
- Compromise / failure of servers
- Compromise or infection of workstations
- Compromised / lost / stolen portable devices (mobile phones, laptops)
- Altered or theft of data (including password files or information considered sensitive - pre- publication, HIPAA, PII, non-disclosure information)
- No detected incidents
- Other

Cybersecurity Concerns

21. What would most improve your project or facility's cybersecurity stature?

Check at most 2

- Advanced security technology (hardware and/or software)
- Cybersecurity steering committee
- Employee/researcher reward / disciplinary systems
- Increased cybersecurity staff
- Larger cybersecurity budget
- Senior Management commitment
- Other

22. What cybersecurity threats are of most concern to your project or facility?

Check at most 2

- Unauthorized or accidental modification of data
- Exposure of confidential or sensitive information
- Loss of availability or sabotage of systems
- Incorrect network/hardware/software configurations
- Email viruses, ransomware or other malware
- Unauthorized, malicious network/system access
- Other

23. Comments - Use this space to record any additional or clarifying comments.

Feedback

24. Thank you for your participation in the CTSC Community Survey. If you have any feedback, please feel free to add comments below.

Appendix B: Tables of Survey Results

Project or Facility Budget

Q1. What is your project or facility's annual budget? [Exclusion is not responsive]

	All	Large Facilities	Big	Small
Range	$100K-$100M	$8M-$200M	$23M-$98M	$100K-$2M
Avg - Mean	$22M	$52M	$60.5M	$1M
Avg - Median	$7M	$50/55M	N/A	$1M
Exclusions	0	0	0	0

Q2. What is your project or facility's annual information technology budget? [Exclusions responded zero or not a separate budget item]

	All	Large Facilities	Big	Small
Range	$0-$65M	$180K-$65M	$3.4M-$4.7M	$0-$1.7M
Avg - Mean	$5.5M	$7.1M	$4M	$1.1M
Avg - Median	$1M	$2M	N/A	$600K
Exclusions	2	1	0	1

Q3. What is your project or facility's annual cybersecurity budget? [Exclusions responded zero or not a separate budget item]

	All	Large Facilities	Big	Small
Range	$0-$2M	$0-$2M	$475K-$900 K	$0-$75K
Range % Budget	0.005%-4%	0.005%-4%	0..48%-3.9%	.75%-3.75%
Avg - Mean	$526K	$442K	$339K	41K
Avg - Median	$80K	$80K	N/A	N/A
Exclusions	6	5	0	1

Q4. What expenses are included in your cybersecurity budget?

	All	Large Facilities	Big	Small
Labor	16	12	2	2
Hardware	16	13	2	1
Software	14	11	2	1
Not Applicable/ Don't Know	2	1	0	1

Project or Facility Attributes

Q5. Is your project or facility an NSF Large Facility?

Yes	15
No	5
Don't know	0

Q6. Do individuals from multiple institutions authenticate to the resources of your project or facility?

	All	Large Facilities	Big	Small
2 or 3	4	4	0	0
More than 3	13	10	1	2
No	2	1	0	1
Don't know	1	0	1	0

Q7. Does your project or facility have a person with defined authority for developing and maintaining a cybersecurity program (e.g., ISO, CSO, CISO)?

	All	Large Facilities	Big	Small
Full-time	4	2	1	1
Part-time	12	10	1	1
No	4	3	0	1
Don't know	0	0	0	0

Q8. Approximately how many FTE's are involved with cybersecurity work (programmatic or operational) within your project or facility?

	All	Large Facilities	Big	Small
None	0	0	0	0
0 to .5 FTE	5	3	0	2
.5 to 1 FTE	4	4	0	0
1 to 2 FTE	4	4	0	0
2 to 3 FTE	1	1	0	0
3 to 4 FTE	3	1	2	0
>4 FTE	2	1	0	1
Don't Know	1	1	0	0

Q9. Does your project or facility develop or maintain software? If so, what policies, processes or tools do you use? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
Coding Standards	12	9	2	1
Interpreted Languages	15	12	2	1
Compiled Languages	14	11	2	1
Source Code Repositories	15	12	2	1
Automated Testing	10	10	0	0
Continuous Integration	10	9	0	1
Static/Dynamic Analysis	1	1	0	0
Issue Tracking / Vulnerability Management	17	14	2	1
Testing Policies	9	7	2	0
Code Signing	7	3	4	0
Automated Documentation	8	8	0	0

Not applicable	2	0	0	2

Cybersecurity Program

Q10. How are cybersecurity policies developed and officially adopted within your project or facility? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
IT or Cybersecurity	13	10	1	2
Governance Board	8	6	2	0
PI or Project Leadership	4	2	1	1
No Process	4	4	0	0
Host Institution	10	8	0	2

Q11. What framework or guidance (if any) has your project or facility adopted for how cybersecurity is done? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
CIS	9	7	1	1
ASD	0	0	0	0
NIST RMF	10	8	1	1
ISO	0	0	0	0
IGTF	0	0	0	0
CTSC Guide	10	9	0	1
None	1	0	0	1

Q12. Who accepts residual cybersecurity risk (i. e., the remaining risk after reasonable cybersecurity controls are established)? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
Cybersecurity person	2	1	0	1
IT Manager	6	5	1	0
System/Process Owner	2	2	0	0
Senior Manager or PI	3	3	0	0
Parent Institution	3	3	0	0
No Process	9	5	1	3
Don't Know	1	1	0	0

Q13. What external cybersecurity requirements (if any) are imposed on your project or facility? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
PII	8	6	1	1
PHI	6	4	1	1
NDA or contractual	9	7	1	1
Classified	3	2	0	1
FISMA	4	4	0	0
CUI	4	4	0	0
Cooperative Agreement	14	14	0	0
None	5	1	1	3
Don't Know	3	0	0	3

Q14. What kind(s) of identity management does your project or facility employ to control access to its resources? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
Parent Institution	6	3	1	2
Project Provided userid/pswd	14	12	1	1
Project Certificate	6	5	0	1
Federated IDM	8	6	1	1

Q15. What programmatic cybersecurity safeguards has your project or facility implemented? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
Maturity Models	3	3	0	0
Strategy, policy or plan	15	12	2	1
Improvement roadmap	12	11	1	0
Documented Standards	13	10	2	1
Inventory critical assets	12	9	2	1
Data classification	7	6	0	1
Cyber incident response plan	15	12	2	1
Disaster recovery plans	12	10	1	1
Periodic awareness training	10	9	1	0
Risk assessments	11	9	2	0
Monitor security intelligence	11	8	2	1
Governance structure	9	6	2	1
External review	5	5	0	0

Parent Safeguards	11	9	1	1
None	0	0	0	0

Q16. What operational cybersecurity safeguards has your project or facility implemented? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
Multi-Factor Authentication	12	8	2	2
Centralized logging	14	11	1	2
Vulnerability management	11	7	4	0
Vulnerability scans	16	12	2	2
Physical access controls	15	11	2	2
Intrusion detection	12	10	1	1
Firewalls	16	13	1	2
Anti-virus, spam, phishing	16	13	1	2
Data Loss prev / encryption	8	6	1	1
Real-time alerts	7	4	2	1
Tabletop exercises	4	2	2	0
Penetration or phishing testing	4	2	1	1
Parent Safeguards	10	6	1	3

Q17. How frequently are patches applied based on the severity rating, either on a fixed maintenance cycle (e.g., monthly) or based on some regular cycle after a patch is released?

2D/1W/1M/3M/>3	All	Large Facilities	Big	Small
Critical	7/9/3/0/0	5/7/3/0/0	1/1/0/0/0	1/1/0/0/0
Important	2/5/8/4/0	1/5/6/3/0	0/0/1/1/0	1/0/1/0/0
Moderate	0/5/6/5/2	0/4/5/4/2	0/0/0/1/0	0/1/1/0/0
Low	0/4/6/4/4	0/3/5/3/4	0/0/0/1/0	0/1/1/0/0

Q18. How many cybersecurity incidents (i.e., any event that puts the confidentiality, integrity, or availability of data or information systems at risk) has your project or facility experienced in the past year?

	All	Large Facilities	Big	Small
1	4	2	1	1
2	3	3	0	0
3	0	0	0	0
>3	5	5	0	0
None	6	4	1	1
Don’t Know	2	1	0	1
Prefer not to answer	0	0	0	0

Q19. For the cybersecurity incidents your project or facility experienced in the past year, what were the programmatic impacts? [Respondents allowed to select more than one.]

	All	Large Facilities	Big	Small
Loss of Reputation	3	3	0	0
Decreased confidence in data	4	4	0	0
Inability to collect / analyze data	5	4	0	1
Interrupt remote access	4	4	0	0
Sanctions or legal	0	0	0	0

action				
Significant cost of recovery	0	0	0	0
Cost of remediation	5	5	0	0
Does Not Apply	8	5	1	2

Q20. For the cybersecurity incidents your project or facility experienced in the past year, which have had the greatest operational impact? [Respondents allowed to select no more than two.]

	All	Large Facilities	Big	Small
Network denial of service	2	2	0	0
Compromise server	3	3	0	0
Compromise workstation	9	8	0	1
Compromised portable device	0	0	0	0
Altered or theft of data	0	0	0	0
No detected incidents	7	4	1	2

Cybersecurity Concerns

Q21. What would most improve your project or facility's cybersecurity stature? [Respondents allowed to select no more than two.]

	All	Large Facilities	Big	Small
Advanced technology	8	5	1	2
Cybersecurity steering committee	3	3	0	0
Reward / disciplinary Systems	1	1	0	0
Increased staff	6	5	0	1

Larger budget	9	8	0	1
Senior management commitment	4	4	0	0

Q22. What cybersecurity threats are of most concern to your project or facility? [Respondents allowed to select no more than two.]

	All	Large Facilities	Big	Small
Modification of data	7	5	0	2
Exposure of sensitive information	4	2	1	1
Loss of availability or sabotage	12	9	1	2
Incorrect configurations	1	1	0	0
Viruses, ransomware, malware	5	5	0	0
Unauthorized access	8	5	2	1