



The Trusted CI Broader Impacts Project Report

June 28, 2018

For Public Distribution

Jeannette Dopheide¹, John Zage², Jim Basney³

¹ Project Lead, jdopheid@illinois.edu

² Project Collaborator, jzage@illinois.edu

³ Co-PI overseer of the project, jbasney@illinois.edu

About Trusted CI

Trusted CI is funded by NSF's Office of Advanced Cyberinfrastructure as the NSF Cybersecurity Center of Excellence (CCoE). In this role, it provides 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 an effective cybersecurity program. Trusted CI achieves this mission through a combination of one-on-one engagements with NSF projects, training and best practices disseminated to the community through webinars, and the annual, community-building NSF Cybersecurity Summit for Large Facilities and Cyberinfrastructure.

For information about Trusted CI , please visit the project website: <https://trustedci.org>

Acknowledgments

This document is a product of the Trusted CI. Trusted CI is supported by the National Science Foundation under Grant Number ACI-1547272. For more information about the Center for Trustworthy Scientific Cyberinfrastructure please visit: <http://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 made available under the terms of the Creative Commons Attribution 3.0 Unported License. Please visit the following URL for details:

http://creativecommons.org/licenses/by/3.0/deed.en_US

Cite this work using the following information:

J. Dopheide, J. Zage, J. Basney, "The Trusted CI Broader Impacts Project Report," Trusted CI, trustedci.org, June 2018. Available: <http://hdl.handle.net/2022/22148>

This work is available on the web at the following URL:

<http://hdl.handle.net/2022/22148>

Table of Contents

Executive Summary	3
1 About the Project	4
1.1 Goals and objectives	4
1.2 Timeline and milestones	4
2 Quantifying Community Impact	5
2.1 The NSF Directorates	5
2.2 Total number of NSF awards impacted by Trusted CI	5
2.3 Comparing NSF awards over \$1 million to Trusted CI's impact	6
2.4 Breaking down Trusted CI's impact by type of interaction	8
2.5 Summit impact by year and Directorate	9
2.6 Analysis of Training by Year and Location	11
2.7 Quantifying current impact: Important takeaways	11
3 Understanding Community Needs	12
3.1 Stakeholder analysis	12
3.2 2017 NSF Community Cybersecurity Benchmarking Survey Report	14
3.3 Analysis of the report of the NSF Large Facilities Cyberinfrastructure Workshop	15
3.4 Understanding community needs: Important takeaways	16
4 Evaluating Current/Potential Strategies for Broader Impact	16
4.1 Evaluate the vision document and potential outreach opportunities	16
4.2 Plotting the vision document's strategic objectives by broadest impact	20
4.3 Sorting the vision document goals by activity type	21
4.4 Evaluating current/potential strategies: Important takeaways	22
5 Recommended Strategy for Broader Impact in Trusted CI	23
5.1 Six Strategies for Broadening our Impact on the NSF Community	23
6 Conclusion	23

Executive Summary

The NSF CCoE is charged to address cybersecurity challenges "affecting small projects, multi-institution collaborations, international collaborations and large facilities."⁴ There are approximately 500 NSF projects each year that are funded at \$1 million or more,⁵ which we believe is a budget level that indicates that they likely develop/use/operate significant cyberinfrastructure with cybersecurity needs. Our estimate to-date is that Trusted CI has interacted with approximately 190 NSF projects (engagements, summits, webinars, mailing lists).⁶ The purpose of Trusted CI's 2018 Broader Impacts project is to develop and implement a strategy to help meet the cybersecurity needs of this broader set of NSF projects (both small and large) and to provide demonstrated value to a significant percentage of NSF projects funded at \$1 million or more.

Recommendations:

Below are six strategies Trusted CI should pursue in the coming years.

1. Fill in gaps in our collection of impact statistics (e.g., affiliation of training attendees).
2. Explore outreach opportunities to the Education and Human Resources (EHR) and Biological Sciences (BIO) Directorates, which are currently underrepresented in our impact metrics.
3. Increase attention on developing and maintaining the website, highlighting the content and services we are already providing. Our materials are only as useful as our stakeholders can discover them. It's helpful to consider different stakeholder perspectives when updating and reorganizing the website.
4. Trusted CI should provide more materials addressing availability and integrity concerns from the community, leveraging external expertise.
5. Trusted CI should document and share its experiences and expertise related to operating a community-focused center of excellence, to benefit other similar organizations.
6. When implementing our 2019-2023 vision⁷, Trusted CI should emphasize outreach as an essential component of each strategic objective.

⁴ NSF CICI solicitation (2015): <https://www.nsf.gov/pubs/2015/nsf15549/nsf15549.htm>

⁵ NSF awards over \$1million:

<https://www.nsf.gov/awardsearch/advancedSearchResult?AwardAmount=5&OriginalAwardDateOperator=Range&OriginalAwardDateFrom=01%2F01%2F2017&OriginalAwardDateTo=01%2F01%2F2018>

⁶ See Figure 1.

⁷ The Trusted CI Vision for an NSF Cybersecurity Ecosystem And Five-year Strategic Plan 2019-2023: <http://hdl.handle.net/2022/22178>

1 About the Project

1.1 Goals and objectives

Goals:

1. Improve Trusted CI's broader impacts through awareness, outreach, etc., for demonstration in Trusted CI reports (e.g., increase to 200 projects interacted with by end of 2018).
2. Develop a Trusted CI strategy for broad impact across "small projects, multi-institution collaborations, international collaborations and large facilities" as input to Trusted CI planning.

To meet the above two goals, the Broader Impacts project had the following four objectives.

Objectives:

1. Quantify Trusted CI impact so far (are we already having a larger impact than we thought? what is our process for making sure we record all impacts, even the small ones like emails to ask@trustedci.org?)
2. Understanding community needs. What are the projects we are missing? What common cybersecurity needs do they have? What unique needs do they have that we haven't considered? Why have we missed these projects? Can we increase awareness of existing guides/templates/etc to make a larger impact? Do the projects we have not connected with want to attend the summit, Can we develop a more compelling "what is Trusted CI" outreach story? What is our process for internally recording community feedback?
3. Evaluate Trusted CI's current and potential strategies for broader impact (conference presentations, training, website, videos, podcasts, emails to new awardees, working through NSF like with large facilities manual and USAP, etc.)
4. Recommend strategy for broader impact in Trusted CI (e.g., identifying new conferences/venues to target for outreach)

Sections 2-5 of this report address each of these four objectives.

1.2 Timeline and milestones

The Broader Impacts project was given a 6 month schedule, resulting in a report that was presented to the Trusted CI All Hands Meeting in June of 2018. The project was launched in January of 2018. The first phase of the project focused on quantifying Trusted CI impact thus far. A lot of time was spent collecting information from registration forms as well as pulling

award data from the NSF site. The next phase was focused on understanding community needs by creating a stakeholder analysis, reaching out to members of the NSF community, and reviewing the findings of the community benchmarking survey. The final phase of the project focused on reviewing the Trusted CI Vision Document comparing its goals to the findings from the previous phases of the project.

2 Quantifying Community Impact

2.1 The NSF Directorates

NSF is divided between seven directorates⁸ that support science and engineering research and education. There are additional NSF directorates that focus on internal matters like outreach and financial management. For the purpose of this Broader Impacts project, the directorates we are focusing on are:

- Biological Sciences (BIO)
- Computer and Information Science and Engineering (CISE)
- Education and Human Resources (EHR)
- Engineering (ENG)
- Geosciences (GEO)
- Mathematical and Physical Sciences (MPS)
- Social, Behavioral and Economic Sciences (SBE)

2.2 Total number of NSF awards impacted by Trusted CI

Defining “impact”

According to the CTSC Final Report, which summarizes Trusted CI’s impact on NSF projects during its initial funding period, our estimate of Trusted CI’s impact so far is 100 projects⁹. We decided to research that number to determine if it was accurate. We defined “impact” as the number of NSF awards that have had an engagement with Trusted CI, had staff that attended a Summit, webinar, or training, since the founding of Trusted CI with NSF award 1234408. We eliminated duplicates to ensure we weren’t double-counting awards that have had multiple interactions with Trusted CI. In addition, we created a separate count of projects that are funded at \$1 million or more because those projects are most likely to operate their own infrastructure and have clear cybersecurity needs.

⁸ See, “Research Areas,” https://www.nsf.gov/about/research_areas.jsp. Accessed 13 February, 2018.

⁹ Center for Trustworthy Scientific Cyberinfrastructure Final Report, 2016
<https://scholarworks.iu.edu/dspace/handle/2022/21073>

NSF awards impacted by Trusted CI

Figure 1 represents Trusted CI's impact on NSF awards. The first column represents total impact across all funding levels. The second column represents total impact across projects funded at \$1 million or more. Both columns are color-coded to show the individual NSF directorates represented in the counts.

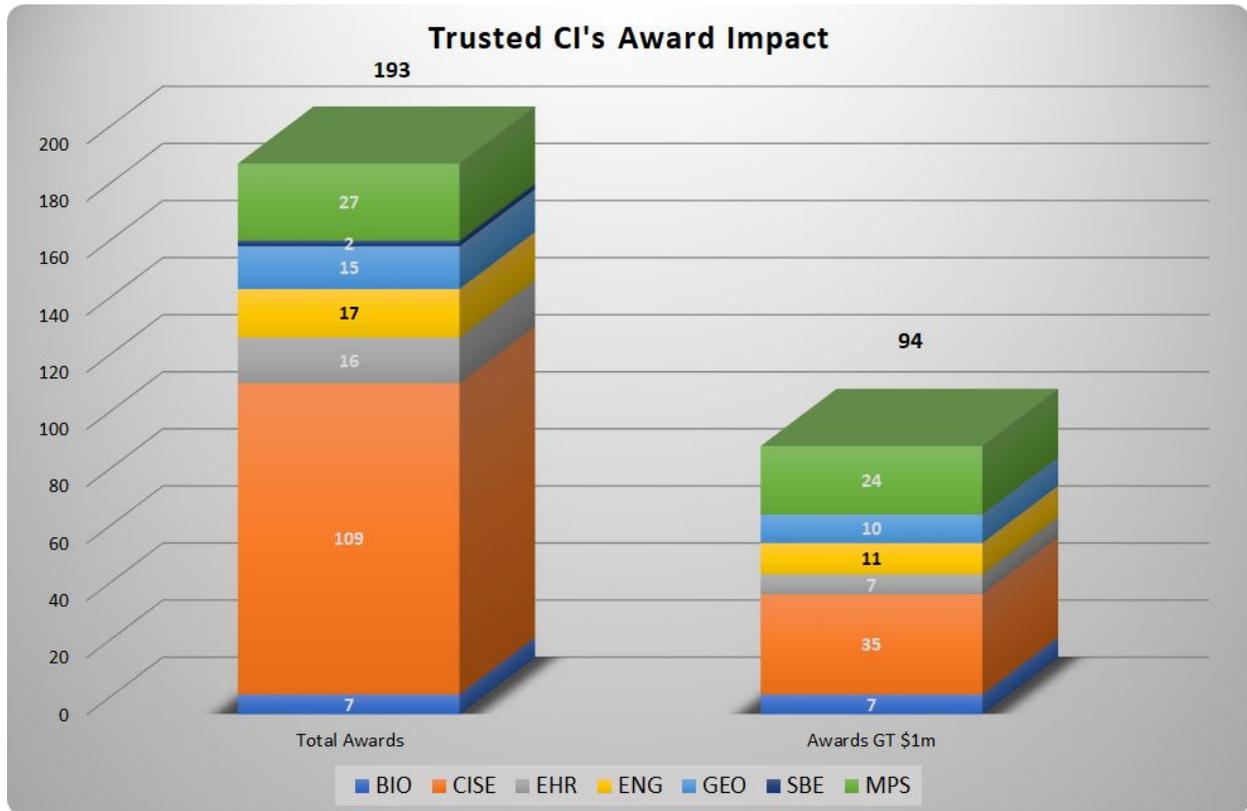


Figure 1. Trusted CI Award Impact

We estimate that approximately 193 projects have interacted with Trusted CI, 94 of them are funded at the target level of \$1 million or more. These numbers indicate that our total impact is greater than the initial 100 project estimate. The Computer and Information Science and Engineering (CISE) directorate makes up a significant amount of our impact to-date.

2.3 Comparing NSF awards over \$1 million to Trusted CI's impact

While it is useful to understand the breakdown of our current impact, it is important to also look at the distribution of NSF funds among the seven target directorates. Figure 2 below compares Trusted CI's impact to the number of awards and NSF funding per directorate (the three values are represented as percentages).

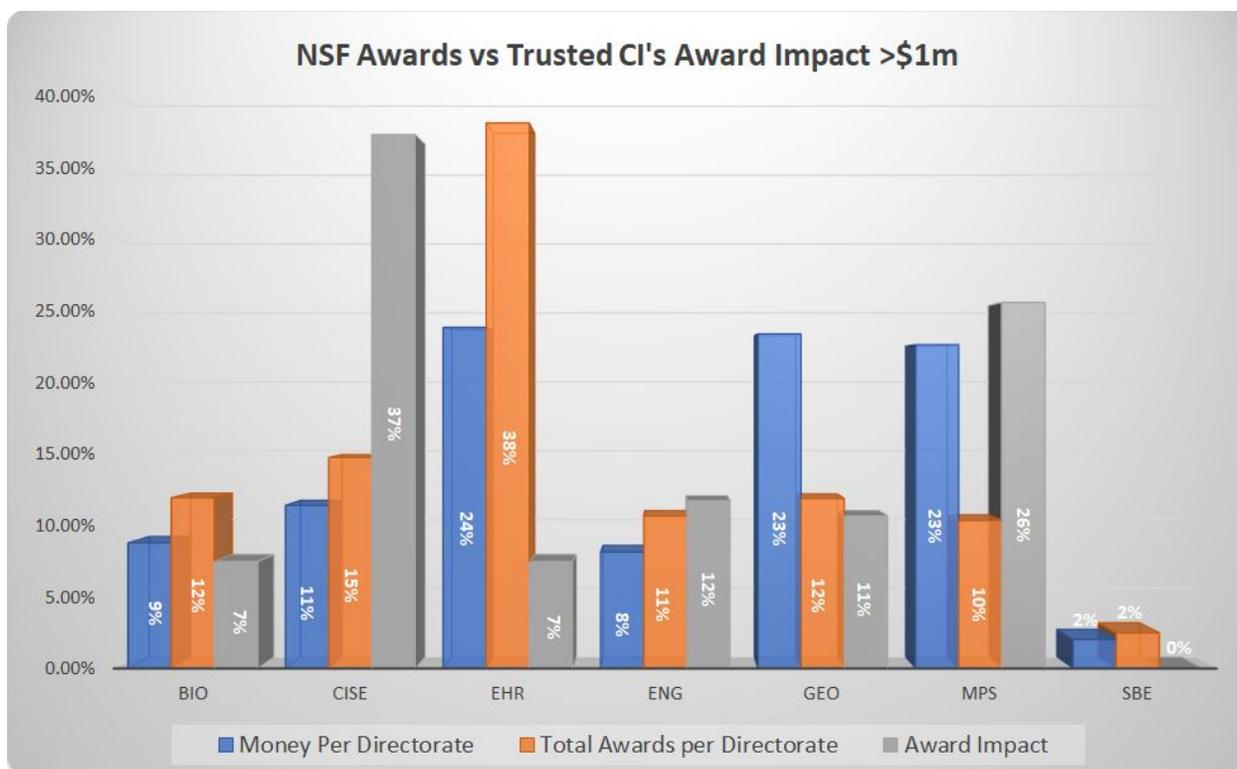


Figure 2. Trusted CI Outreach vs NSF Awards #/\$'s per Directorate as a percentage of total

The directorates with the largest share of NSF award funds are Education and Human Resources (EHR), Geosciences (GEO), and Mathematical and Physical Sciences (MPS). Both GEO and MPS have significantly fewer awards compared to EHR and yet still have high dollar grants. We determined that this difference is due to large research projects (telescopes, the gravitational-wave observatory, particle accelerators, etc.) that are funded under those directorates.

The Education and Human Resources (EHR) directorate supports STEM education for the preparation of future scientists, engineers, and mathematicians. EHR represents a large percentage of awards and NSF funding, and yet Trusted CI's impact on this directorate has not yet been very significant. This may indicate an opportunity to make a bigger impact in the future.

And, as demonstrated in the previous chart, Trusted CI's outreach effort has a significant impact on Computer Information Science and Engineering (CISE). Our impact to-date on Social, Behavioral and Economic Sciences (SBE) does not appear to be significant, though not unreasonably out of alignment with their share of NSF funding.

2.4 Breaking down Trusted CI's impact by type of interaction

We also reviewed Trusted CI's impact depending upon the type of interaction (engagement, attending the summit, and webinar).

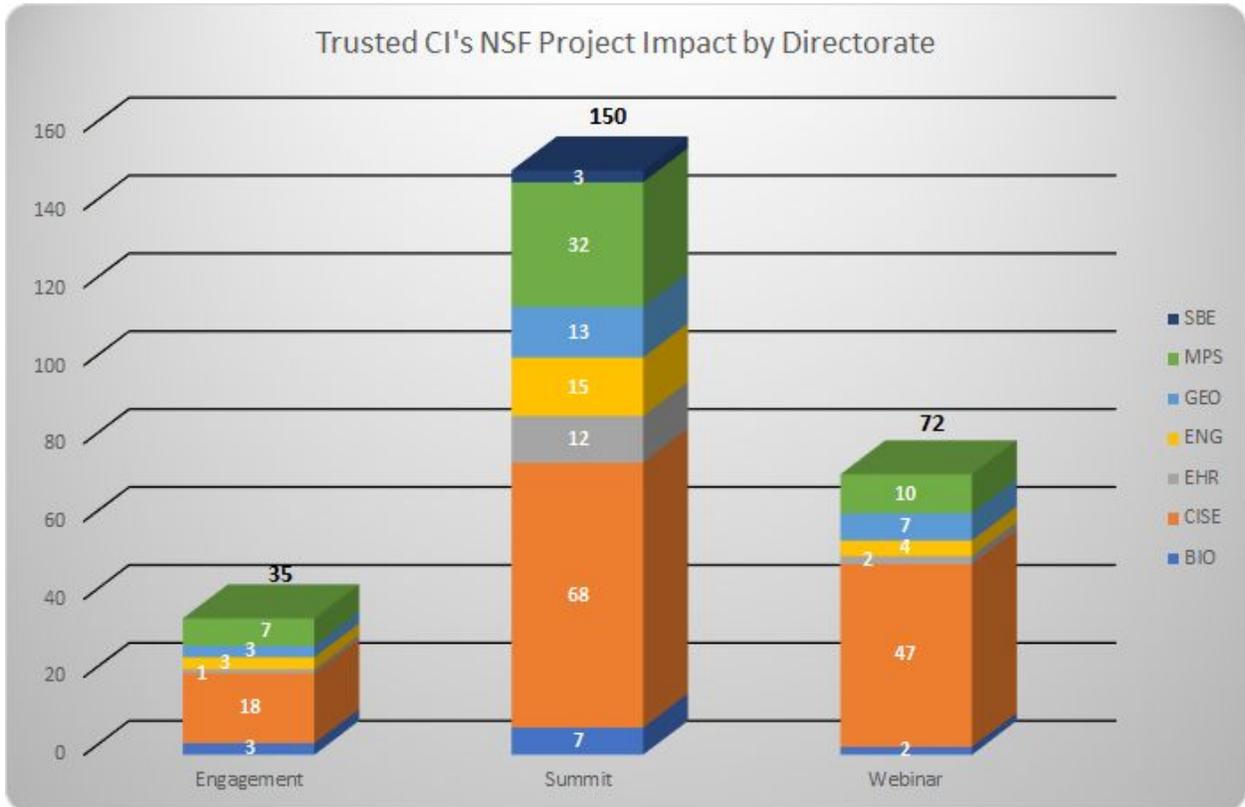


Figure 3. Trusted CI's NSF Project Impact by Directorate

For the purposes of comparison, Figure 3 shows Trusted CI's project broken down by type and NSF Directorate. Our greatest outreach impact is the NSF Summit, followed by the webinar series, and engagements.

2.5 Summit impact by year and Directorate

Figure 4 breaks down the summit attendees by year and NSF Directorate. We did not collect NSF project names from the 2013 Summit attendees, which is why it is not listed as a column in this graph. Prior to 2015 the Summit was invitation only, with one or two invitations sent per project. In 2015 the planning committee removed the registration restriction and permitted more than two people per project (provided seating was available). This change in policy accounts for the dip in number of projects despite registration attendance slowly increasing. Note that in 2016 we did not see representation from the Biological Sciences Directorate. This could be an opportunity to review our program to highlight topics of interest to the BIO Directorate.

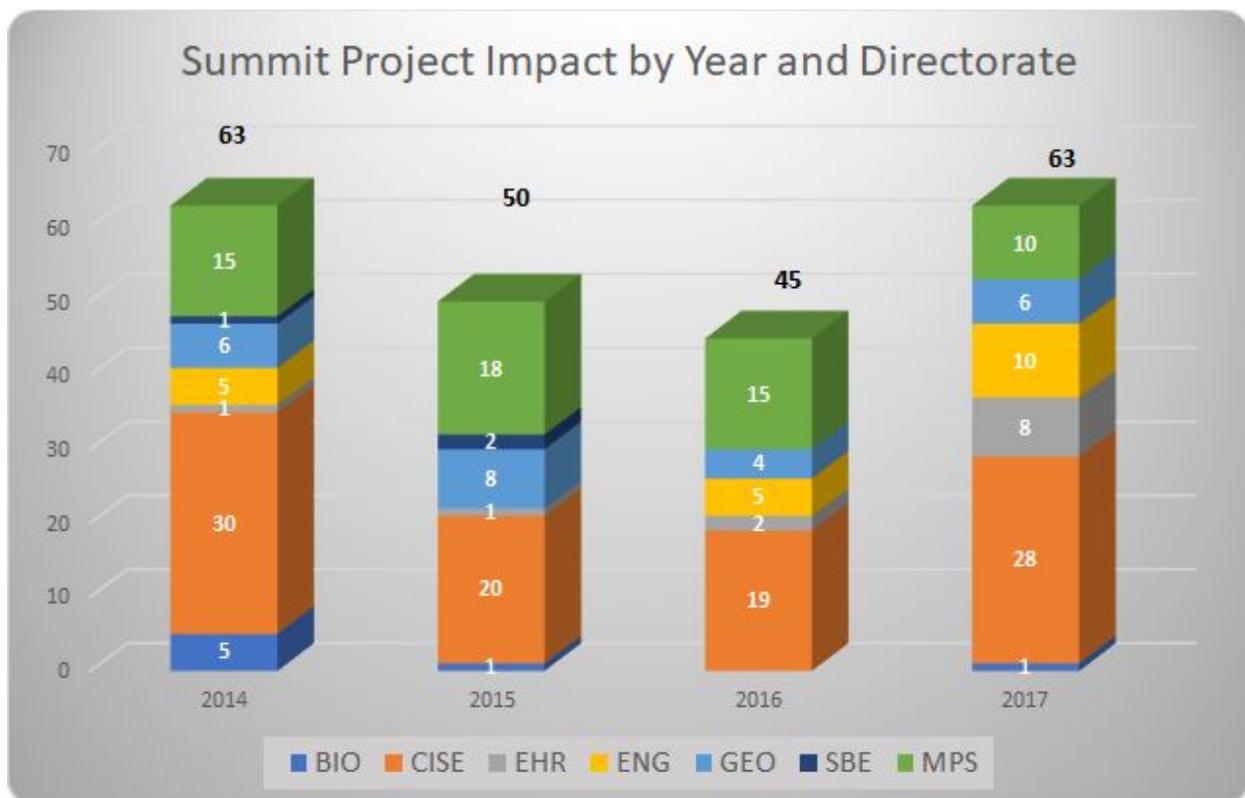


Figure 4. Summit Project Impact by Year and Directorate

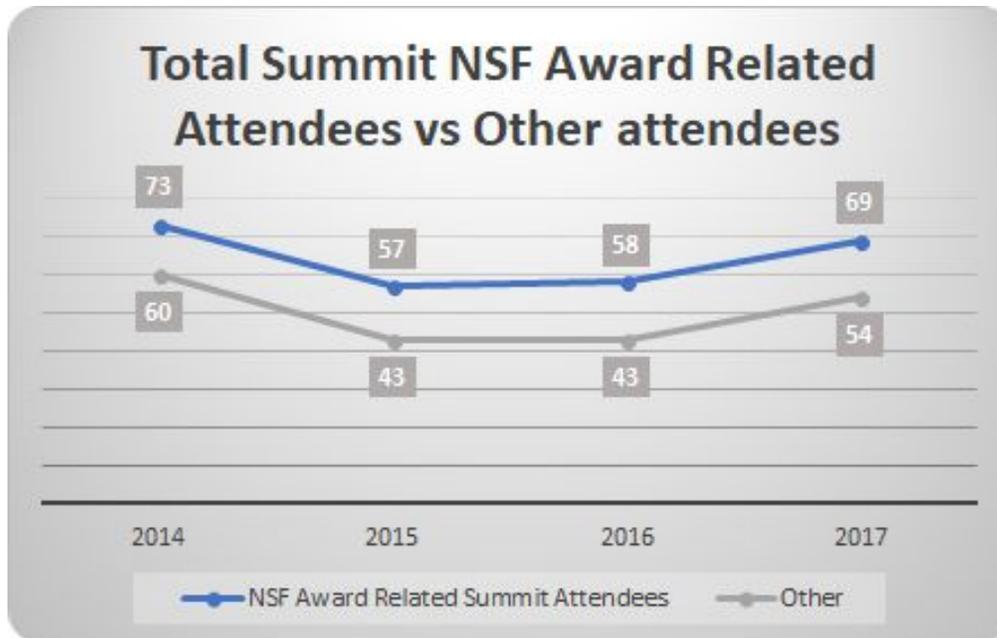


Figure 5. NSF Summit Total Project Impact vs Other attendees

Figure 5 is a line graph that tracks the NSF Summit attendance, split between who was and was not affiliated with an NSF project¹⁰. The “others” stay consistently below the number of attendees who are affiliated with NSF awards. This is as expected because the Summit targets NSF Awardees but still welcomes non-NSF projects to attend (Lawrence Livermore National Lab, National Institutes of Health, ESNet). In comparison to other Trusted CI activities, the Summit has the broadest impact across NSF, including attendees from 12 EHR projects to-date, indicating that the Summit plays an important role in broadly impacting NSF projects.

¹⁰ NSF program officers were categorized as “other” in this table due them not being funded on a specific NSF grant, but rather as direct employees of NSF.

2.6 Analysis of Training by Year and Location



Figure 6. Training hours by Year and Source

Figure 6 is a summary of the total hours of training given in a year, broken down by the NSF Summit and other training events Trusted CI was invited to present. Year 2017 saw a significant increase in trainings offered due to the Cal Poly Pomona Scholarship for Service Engagement as well as other trainings in software assurance, log analysis, and incident response. More outside organizations are requesting our training services, which reinforces our impact on the NSF community.

2.7 Quantifying current impact: Important takeaways

We believe there are many opportunities for better tracking of awardee interactions with Trusted CI. Below are a few suggestions:

- Requesting NSF grant number in webinar registration form.¹¹
- We do not reliably collect training attendees' names or NSF affiliations during non-Summit training events. Figure 6 above shows our training effort has significantly increased over the past two years. These are missed data points.

¹¹ Added as of February, 2018

- Aside from web page views, we do not have much data on the customers coming to our website. It may be helpful to add a popup with optional fields for email or NSF project, when downloading a guide or report template.
- Our webinar attendees overwhelmingly represent the CISE directorate. There may be topics or speakers from the other directorates that also are of interest to our audience. For example, we could solicit a webinar presentation about cybersecurity concerns unique to Engineering projects.

There are also a number of observations about the data analysis that should be highlighted:

- The Education and Human Resources Directorate (EHR) represents a large percentage of awards and NSF funding, and yet Trusted CI's impact on this directorate has not yet been very significant.
- In 2016 we did not see representation at the Summit from the Biological Sciences Directorate (BIO). This could be an opportunity to review our program to highlight topics of interest to the BIO Directorate.
- More organizations are requesting our training services at their events, which reinforces our impact on the NSF community.
- Trusted CI has provided cybersecurity services to 193 NSF projects to-date, across all 7 NSF research and education directorates. While Trusted CI's engagements have a significant impact on a small number of projects, our summit and webinar activities are already having a broad impact across a larger number of projects.

3 Understanding Community Needs

3.1 Stakeholder analysis

A stakeholder is anyone interested in the outcome of a project. Table 1 breaks down the project stakeholders, ordered by priority, and lists what they want and what we (Trusted CI) can provide. It should be noted that the items in "What we can provide" section are not exclusive to that stakeholder group, but rather the services that are most applicable to that stakeholder group.

Table 1.Trusted CI stakeholder analysis chart

Stakeholder	What they want	What we can provide
Trusted CI Program Officer	To quantify the value that Trusted CI provides	Better tracking of impact statistics
Trusted CI Staff	To make a difference / big impact. They work directly with NSF project members and are invested in their success.	More feedback on priorities and ways to make a bigger impact.
NSF Projects > \$1m	Need help with their security	Engagements, training, guides, opportunities to collaborate (NSF Summit, mailing lists), webinars
NSF Large Facilities	Specific security requirements in their contracts with NSF	Large Facilities manual
NSF Large Facility Security Officers	Care about securing their facilities, value communication with peers	Large Facilities manual , facilitate interaction between projects
Higher Ed IT Professionals	Care about campus security and the integration of NSF projects into campus cyberinfrastructure	Educate regarding research project interaction and cybersecurity needs
NSF Projects < \$1m	Have limited resources for security, need practical cybersecurity resources	Training, guides, opportunities to collaborate (NSF Summit)
Students	Workforce development	Training, access/funds to attend the Summit
NSF Program Officers	Want awardees to have good security, to represent the NSF in a positive light	Increase their awareness of Trusted CI's services, use their access to contact awardees
Other cybersecurity professionals willing to share expertise/tools ¹²	An opportunity to spread their knowledge or open-source project among NSF community	Host their training at the NSF Summit, host webinars, create working groups, make connections with projects that need help

¹² These are people who give training (Bro Project, Security Onion, control system security), IAM providers (Globus, CILogon), security consultants (especially those who target NSF projects).

Other people looking for cybersecurity help ¹³	Free resources for their individual cybersecurity needs	Post approved content to the website
---	---	--------------------------------------

3.2 2017 NSF Community Cybersecurity Benchmarking Survey Report

In 2017 Trusted CI issued its annual community benchmarking survey to collect and aggregate information about the state of cybersecurity for NSF projects. There were 20 survey responses, 15 of which were from Large Facilities. We reviewed the report¹⁴ with the intent of identifying potential areas for broader impact.

Below are a few quotes from the document and accompanying observations:

- *Software: A clear majority use bug management, code repositories, and both interpretive and compiled programming languages*
 - We have a number of Trusted CI staff with experience educating people on software best practices. We could do more to promote the content we have by adding it to the website or drawing more attention to it. Example: How to address the challenges with picking software at large facilities.
- *Cybersecurity frameworks: NIST RMF, CIS Critical Security Controls, and Trusted CI Guide had the most adoption with 10, 9, and 10, respectively*
 - Our website landing page could be better utilized to bring attention to the Trusted CI Guide. Also, it would be helpful to explain when to use the Trusted CI Guide vs the other guides listed. The publication of the second version of the Guide is a great opportunity to address these concerns.
- *Incidents: Most common concern of breaches is “cost of remediation,” but reputational harm, and loss of access/integrity are also somewhat common (among those who suffered breaches)*
 - Our Incident Response content is mostly contained in slideshow presentations that have to be individually opened and reviewed. We could do more to bring that content to the forefront of the site (Example: Top ten steps to take after a security incident)
- *Incidents: Workstation compromises have the biggest operational impact.*
 - Craig Jackson and Susan Sons have written a presentation on Cybersecurity for Smaller Projects that could address some of these concerns.

¹³ These people are affiliated with non-NSF science projects, cybersecurity professionals not affiliated with NSF projects, campus IT staff, international and small businesses who find our resources online.

¹⁴ 2017 NSF Community Cybersecurity Benchmarking Survey Report: <http://hdl.handle.net/2022/22171>

- *Areas for improvement: Increased budgets and Advanced Security Technologies were by far the most common responses*
 - Craig Jackson and Bob Cowles have some experience in the topic of cybersecurity budgeting. Perhaps this is a topic that could be pursued as a webinar or seminar during the NSF Cybersecurity Summit
- *Fears: By far the biggest fear was loss of availability*
 - Trusted CI staff should reach out to contacts at organizations like ESNet and Internet2 to present a webinar on topics that include denial of service attacks, web access failures, ransomware, etc.

3.3 Analysis of the report of the NSF Large Facilities Cyberinfrastructure Workshop

The NSF Large Facilities Cyberinfrastructure Workshop was held in September of 2017 and produced a report¹⁵ that a couple references to Trusted CI and its relationship with the large facilities community. “The overarching goal of the workshop was to enable direct and synergistic interactions among the NSF large facilities and the CI communities to jointly address the CI needs as well as the sustainability of the CI of existing and future large facilities.” Below is a summary of noteworthy excerpts from the report.¹⁶

- Under the “Key Findings” Section:
 - *“There is a critical lack of a focused entity that could facilitate interactions and sharing across facilities. A model such as that used by the NSF-funded Center for Trustworthy Scientific Cyberinfrastructure (CTSC) was explicitly and repeatedly noted as an effective model that should be explored to address this gap.”*
- Under “Recommended Actions” Section:
 - *“Establish a center of excellence (following a model similar to the NSF-funded Center for Trustworthy Scientific Cyberinfrastructure, CTSC) as a resource providing expertise in CI technologies and best practices related to large-scale facilities as they conceptualize, start up, and operate.”*

Trusted CI should offer assistance to the large facilities leadership team in their plan to form a center of excellence. This is a great opportunity to address strategic objective 1.3 in the vision document: Build the community needed for the NSF cybersecurity ecosystem.

¹⁵ Report from the NSF Large Facilities Cyberinfrastructure Workshop:
<http://facilitiesci.org//images/facilitiesci-workshop-report-11-17.pdf>

¹⁶ Note Trusted CI is referred to as CTSC in the report. The project hadn’t announced its new name until March of 2018.

3.4 Understanding community needs: Important takeaways

The community benchmarking survey provided the most helpful insights regarding quantifying the needs of the NSF community. In summary:

- There are many opportunities to improve the website and access to information that may be available in slideshows and presentations, but not readily available.
- Publishing the second version of the Trusted CI Guide is an opportunity to re-evaluate how the guide is presented to visitors to our site.
- There are existing resources on practical cybersecurity for smaller projects and cybersecurity budgeting that could be further developed and promoted to the community.
- Trusted CI should reach out to organizations with operational experience in denial of service, web access failures, ransomware, etc. to share their knowledge and experience with the NSF community.
- Trusted CI should offer assistance to existing and planned centers of excellence.

4 Evaluating Current/Potential Strategies for Broader Impact

4.1 Evaluate the vision document and potential outreach opportunities

The document, “The Trusted CI Vision for an NSF Cybersecurity Ecosystem And Five-year Strategic Plan 2019-2023,” (the “vision document”) lays out a plan to support an NSF cybersecurity ecosystem. This document lists specific strategic objectives that will define the major projects and staffing activities for the next four years. We have reviewed the vision document in order to gain insights into the project and its potential for broader impacts. Below is the list of the objectives outlined in the vision document, potential outreach opportunity, and goal, for each objective.

Table2.The Vision document, outreach analysis

#	Strategic objective (brief description)	Outreach opportunity	Outreach goal
1.1	Develop and support the adoption of the NSF Cybersecurity Framework	New materials will be promoted on the website, webinar, and presentations	Make NSF project staff aware that the framework (Guide) exists.
1.2	NSF Community awareness	Email campaigns, presentations, and flyers to target the intended demographic	Make NSF project staff aware of Trusted CI resources and activities.
1.3	Build the community needed for the NSF cybersecurity ecosystem	Continue promoting the Summit.	Help NSF project staff communicate with each other.
1.4	Continue to deepen the community's understanding of trustworthy science	Promote webinars and other resources that PIs can apply to their NSF projects.	Awareness of the Trusted CI "flexible approach".
2.1	Effective assistance and sustainability	Continue promoting the engagement application during the two application periods per year.	Awareness of engagement application opportunities. Awareness of engagement outcomes.
2.2	Define metrics and track progress	Encourage more survey respondents and requests for community feedback.	Need NSF projects to participate in metrics definition and collection. Share aggregate metrics back to the broader community (not just summit attendees).

3.1	Improve the security of NSF cyberinfrastructure	Try to find more venues for training opportunities, promote the secure coding modules.	Raise awareness of training materials.
3.2	Coordinate with the NSF CSRC	Promote CSRC to Trusted CI community	Avoid confusion of roles between the centers. Interact with community effectively.
3.3	Service coordination and delivery	Identify and reach out to third-party developers who have the potential to positively impact the NSF community.	Need broad awareness of services to get broad adoption to make the economies of scale work. Find out what services are needed.
3.4	Build a national community around cybersecurity for research	Promote Trusted CI materials/services to outside organizations.	Increase awareness of Trusted CI products to non-NSF community. Help NSF community learn about products produced outside.
4.1	Workforce development and training	Continue training programs.	Increase awareness of training. Increase awareness of CI career development opportunities.
4.2	Workforce inclusion and recruitment.	Promote Trusted CI or refer jobs/internships to non-traditional forums, mailing lists.	Increase awareness among minorities and underrepresented groups.

4.3	Outreach to higher education	Attend events hosted by Coalition for Academic Scientific Computation, the CaRC Consortium, and Advanced Cyberinfrastructure Research and Education Facilitators	Increase awareness on campus as a force multiplier of Trusted CI efforts (so campus security folks can help campus researchers).
4.4	Build a network for cybersecurity fellows.	Panel discussions with fellows, potential webinar topic.	Bridge the gap between researchers and cybersecurity practitioners. Fellows provide a force multiplier.
4.5	Cybersecurity transition to practice	TTP panel discussion has been proposed for Summit, host a TPP webinar/presentation on success stories.	Bridge the gap between research and application. Increase the researchers' awareness of needs and increase the practitioners awareness of available solutions coming out of the research community.

4.2 Plotting the vision document's strategic objectives by broadest impact

Figure 7 sorts the strategic objectives into groups with the narrowest to broadest impact. The top level represents a specific targeted subject with an impact that is narrow in the immediate aftermath. Examples include our engagements, or the plans to coordinate with the CSRC. The second level represents goals where the subject of the immediate impact is Trusted CI and affects our projects or processes. Examples include developing metrics or transition to practice (TTP). The third level represents the Trusted CI community. Examples include projects we impact through community awareness or training workshops. Lastly the bottom level represents goals with the broadest impact in the immediate aftermath. Examples include initiatives that are publicly and freely available to anyone who visits our website (the Guide) and expanded access to our Cybersecurity Summit. Arrows were added to help indicate greater impact has less focus and vice versa.

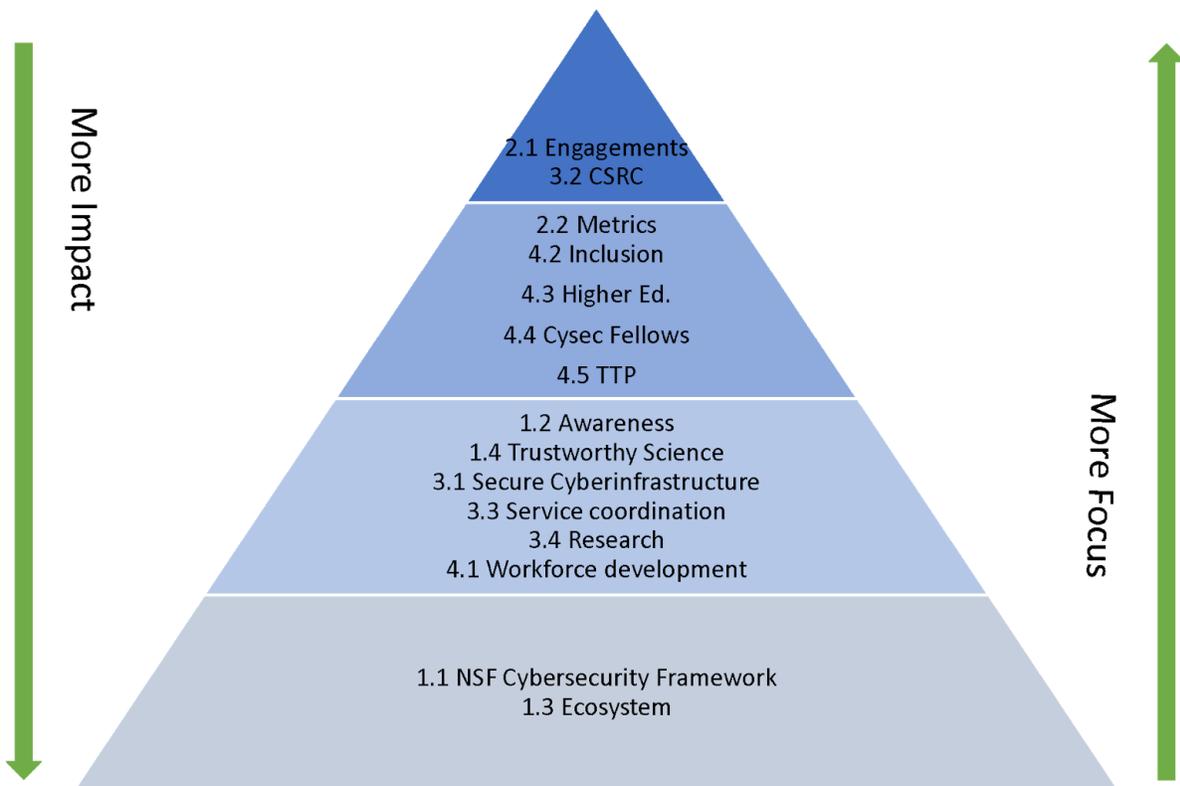


Figure 7. Plotting the vision document's strategic objectives by broadest impact

4.3 Sorting the vision document goals by activity type

Trusted CI tracks and groups its projects into four activity types: Engagements (i.e., our one-on-one engagements with NSF projects), Outreach (presentations, webinar series, collaborations with events like PEARC, etc.), Training (software assurance, Trusted CI guide training, etc.), and Community Leadership (the benchmarking survey, Summit, large facilities manual, etc.).

With these activity groupings in mind, Table 3 is a chart that maps the goal, in a very general sense, to an activity type.

Table3. Categorizing the Vision document’s strategic objectives by Trusted CI activity type

Strategic objective	Activity type
1.1 NSF Cybersecurity Framework	Community Leadership
1.2 NSF Community Awareness	Outreach
1.3 Build community for NSF security ecosystem	Outreach
1.4 Deepen community understanding of trustworthy science	Outreach
2.1 Effective assistance and sustainability	Engagements
2.2 Definite metrics and track progress	Community Leadership
3.1 Improve security of NSF cyberinfrastructure	Training
3.2 Coordinate with the NSF CSRC	Community Leadership
3.3 Service coordination and delivery	Outreach
3.4 Build a natural community around cybersecurity for research	Outreach
4.1 Workforce development and training	Training
4.2 Workforce inclusion and recruitment	Outreach
4.3 Outreach to higher ed.	Outreach
4.4 Build a network of cybersecurity fellows	Community Leadership
4.5 Cybersecurity TTP	Community Leadership

Figure 8 below converts the distribution of strategic objectives to activity types into a pie chart. It should be noted that the distribution is not weighted and doesn't account for the effort necessary to accomplish the objective. However it is somewhat illuminating to see that Community Leadership and Outreach take up the overwhelming share of the objectives.

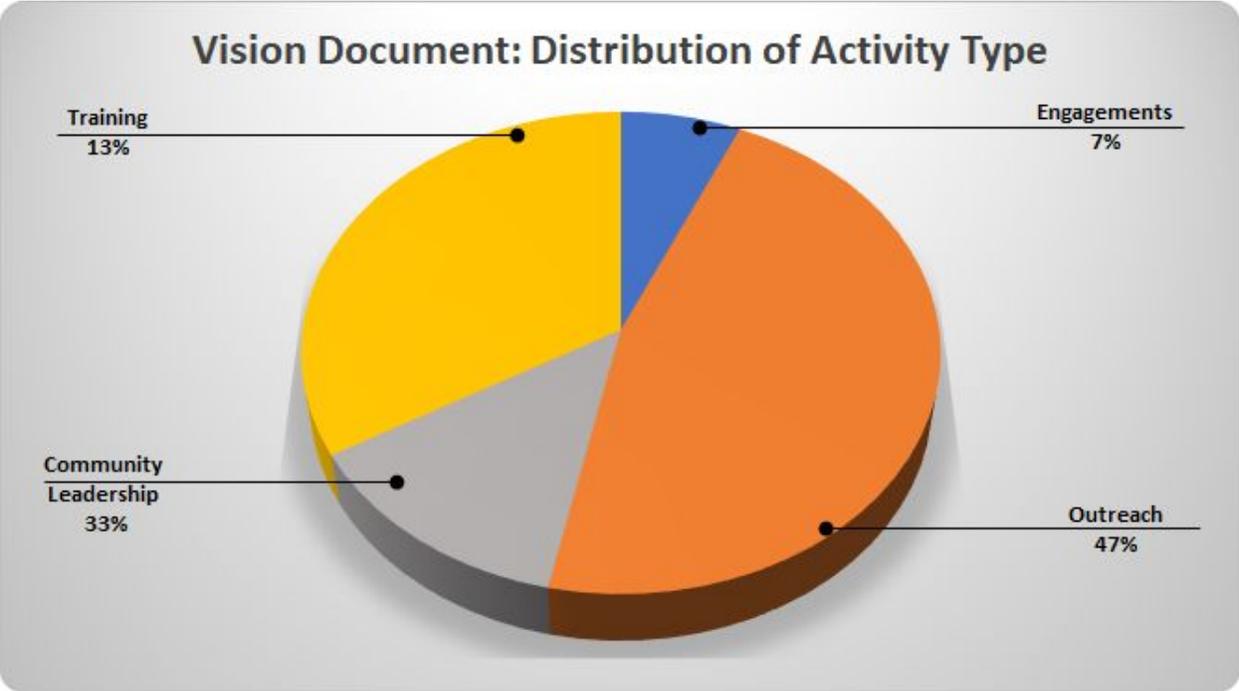


Figure 8. Vision Document: Distribution of Activity Type

4.4 Evaluating current/potential strategies: Important takeaways

- The Trusted CI vision document's objectives can be interpreted as a method for identifying projects with varying degrees of impact (Figure 7). This may be helpful when gauging the balance between strategic objectives and organization effort.
- The Trusted CI vision document lays out a number of goals with outreach opportunities and represent a dramatic shift toward community leadership and outreach initiatives, i.e. broader impacts.

5 Recommended Strategy for Broader Impact in Trusted CI

5.1 Six Strategies for Broadening our Impact on the NSF Community

This report represents the most thorough analysis of our impact on the NSF community to date. Some observations have been reassuring while others have revealed weak spots in our outreach efforts. Below are six strategies Trusted CI should pursue in the coming years.

1. Fill in gaps in our collection of impact statistics (e.g., affiliation of training attendees).
2. Explore outreach opportunities to the Education and Human Resources (EHR) and Biological Sciences (BIO) Directorates, which are currently underrepresented in our impact metrics.
3. Increase attention on developing and maintaining the website, highlighting the content and services we are already providing. Our materials are only as useful as our stakeholders can discover them. It's helpful to consider different stakeholder perspectives when updating and reorganizing the website.
4. Trusted CI should provide more materials addressing availability and integrity concerns from the community, leveraging external expertise.
5. Trusted CI should document and share its experiences and expertise related to operating a community-focused center of excellence, to benefit other similar organizations.
6. When implementing our 2019-2023 vision, Trusted CI should emphasize outreach as an essential component of each strategic objective.

6 Conclusion

One of the most rewarding aspects of the broader impacts project has been reviewing Trusted CI's numerous accomplishments the in six years since the project began. Members of over 150 NSF projects have attended our NSF Summit. We have conducted 35 engagements. We hosted or presented over 250 hours of training seminars. Members of 70 NSF projects have attended our webinars. When totaling these efforts overall, we have impacted over 190 NSF projects, almost 100 of them are funded at \$1 million or more. Our role in the NSF community is stable and growing. Trusted CI's next five years present an exciting challenge to take what we have learned thus far and continue to support the cybersecurity needs of NSF projects.