Review of Security Documents Governing DesignSafe-CI's Cyberinfrastructure

Current State and Opportunities

5 October 2017

For CTSC Distribution to Nathaniel Mendoza, DesignSafe-CI

Andrew Adams[1], Terry Fleury[2]

[1] Engagement Lead, akadams@psc.edu

[2] tfleury@illinois.edu

About the NSF Cybersecurity Center of Excellence

The mission of CTSC, the NSF Cybersecurity Center of Excellence, is to provide the NSF community with a coherent understanding of cybersecurity, its importance to computational science, and what is needed to achieve and maintain an appropriate cybersecurity program.

Table Of Contents

Executive Summary

DesignSafe has a fairly mature security program in place, thus, the purpose of this engagement was focused on reviewing the security documents governing their cyberinfrastructure (CI) in order to gauge the coverage or completeness of these documents compared to best practices for each of the experimental facilities (EFs).

This report explains the purpose, scope, and process of the engagement (Section 1); details observations regarding the security documents that were provided by DesignSafe (Section 2); and provides opportunities for improving those documents or other aspects of DesignSafe's CI (Section 3).

1 Engagement Background & Process

DesignSafe-CI (DesignSafe) is a component of The Natural Hazards Engineering Research Infrastructure (NHERI) funded by multiple grants from the NSF, most recently #1520817 under a Cooperative Agreement through the Div Of Civil, Mechanical, & Manufact Inn (CMMI)[3]. From DesignSafe's web site:

"DesignSafe is the CI component of the NHERI collaboration. DesignSafe embraces a 'cloud' strategy for the 'big data' generated in natural hazards engineering research. It supports research workflows, data analysis and visualization."

CTSC's and DesignSafe's primary goal and objective for this engagement was to gauge the thoroughness and coverage of the DesignSafe security program. This was accomplished by CTSC reviewing the security documents for DesignSafe and its EFs (recorded in an artifact inventory[4]), and comparing those to best practices, specifically chosen from the "Guide to Developing Cybersecurity Programs for NSF Science and Engineering Projects" (https://trustedci.org/guide/). The existence and detail of each security control listed in the guide for each security document within the artifact inventory was recorded in a matrix, referred to as the Document Summary for Each Experimental Facility (EF)[5].

A secondary objective of this engagement was to produce potential improvements, or a list of "opportunities for improvement". Using the matrix and its observed strengths and weaknesses of each document, CTSC and DesignSafe strategized on what documents needed attention, and how best to prescribe that work and/or resources involved.

During the course of the engagement CTSC had a interactions with DesignSafe staff; they provided necessary information, including, but not limited to:

- Conference Call with Nathaniel Mendoza on Aug 9, Aug 30, Oct 4, Oct 25 (2017)
- Security documents (listed here) were provided

2 Observations

The data (i.e., empirical observations) reported for the security policies of each EF in the summary matrix show a significant spread of completeness or coverage of best practices (security controls), specifically, roles and contact information, acceptable user policy, access control or account and authentication management, disaster recovery, incident response, information resource use policy and classification policy, logging/auditing and patch

[3] https://www.nsf.gov/awardsearch/showAward?AWD_ID=1520817
[4] https://docs.google.com/spreadsheets/d/1Es77znG6z1HrAtEcNlQoLS4iI_q9ydXhVTfKPJRgCpc/
[5] https://docs.google.com/spreadsheets/d/1LGgmy3xOsmqNt4K1OWcM94VXYtswAIoLXc12Ls5wqrs/

management, mobile computing policies, password policy, personnel exit processes, physical security, risk assessment processes, training and awareness, and vulnerability scanning.

Instead of looking at each site individually, we decided that a more effective strategy would be to group the EF's (i.e., their associated security documentation) in three categories, high, medium and low, depending on the number of non-detailed (reported by green cells in the matrix) security controls.

Note, the observations below do not reflect the current the security at a site, i.e., we are not implying that University of Texas at Austin is more secure than UC Berkeley's SimCenter, just that the policy documents in place and available to us for Austin are more thorough and detailed than at Berkeley.

High (or Thorough Coverage)

1) **The University of Texas at Austin** leads all sites with no security controls missing, and only two (access control and vulnerability scanning) not being well described/defined.
2) **Florida Int'l University** also scored well covering in detail nine best practices and only omitting information resource policy, personnel exit processes and vulnerability scanning, with incomplete mention of disaster recovery and logging/auditing and patch management.

Medium (or Good Coverage)

1) **UC Davis** provided decent information regarding all of its policies, thoroughly covering six of the best practices, and affirming (with little detail) another four. However, no policies were provided for acceptable user, information resource and classification, mobile computing, and personnel exit.
2) **Lehigh University** provided detailed information for five security controls and mentioned another five controls. The security documentation lacked any reference to account mangement, information resource and classification, mobile computing, and personnel exit processes.
3) **University of Florida** addressed seven best practices in their policies, with a casual mention to disaster recovery. Missing from their documentation were acceptable use policy, incident response, logging/auditing and patch management, personnel exit processes, physical security, training and awareness, and vulnerability scanning.
4) **DesignSafe-CI** included sufficient information regarding five best practices, touched on a sixth and partially mentioned four others. Topics omitted include, acceptable use policy, disaster recovery, information resource and classification, mobile computing, and personnel exit processes.
5) **UC San Diego** could just have easily been fitted under *Low* only three best practices mentioned in detailed, two more weakly, and another four only in passing. There was no

acceptable use policy, information resource and classification, mobile computing, or personnel exit policy mentioned.

Low (or Poor Coverage)

1) **Oregon State University** provided an Information Security Program summary for the College of Engineering. No mention was made of the O.H. Hinsdale Wave Research Laboratory. The documentation relied heavily on university policies, some of which were mentioned in referenced links.
2) **University of Washington** coverage in their security documentation was poor. Only mentioning risk assessment, and that through a link to the university's policy.
3) **UC Berkeley (SimCenter)** has the least detailed security documentation, with only one security control (training & awareness) being defined (as through the university), but failing to even provide a link for that.

3 Opportunities For Improvement

Based on the completeness matrix's implied strengths and weaknesses of each security document provided, DesignSafe and CTSC are listing the following opportunities for improvement:

1) Gap analysis based on this assessment will be acted upon and each site will be required to take corrective action.
    a) This analysis will be placed on the internal DesinSafe wiki for all EF's to review.
2) This assessment will also be disseminated to the management team of DesignSafe to ensure that these corrective actions are taken. This will be sent by November 1, 2017.
3) These gaps will be re-evaluated internally at design safe to ensure compliance and will be looked at in 90 days from the end of this engagement.

4 Areas for Future Engagements

DesignSafe has suggested that a follow-up engagement to re-evaluate their progress in enhancing their documentation would be desired. The review performed by CTSC would be straightforward in evaluating the state of DesignSafe's updated security documents. This form of engagement, however, would be more mutually beneficial to both parties if DesignSafe could present plan to share the effort and methods they pursued in addressing the observations outlined above (see Section 2) to their security documents with other large facilities.