ADVANCING CYBERSECURITY SINCE 1985

ACSA

APPLIED COMPUTER SECURITY ASSOCIATES

STATEMENT REGARDING NATIONAL SCIENCE FOUNDATION FUNDING CUTBACKS

Applied Computer Security Associates (ACSA), a U.S. 501c3 non-profit, is one of the seminal associations in the field of Computer Security, now known as Cybersecurity, having started the Annual Computer Security Applications Conference (ACSAC) in 1985. We have watched the recent cutbacks at the National Science Foundation (NSF) and assessed them both for the impact on ACSAC and other events we operate, and on the broader field as a whole.

ACSA believes that these cutbacks will severely impact the field of cybersecurity research and may very well drop the United States from the top tier of cybersecurity research nations. Further, as researchers educated through these grants move from academic institutions into the American industrial, government, and academic workforce, the weakened research and skill sets will put American industry at a disadvantage, both in terms of competitive innovation and protection from adversarial attack.

Specifically, we see impacts in the following areas:

1. **Reduced attendance at conferences:** NSF will provide less funding for students to attend conferences, both directly through conferenceships and indirectly from grants covering travel. Attendance at conferences is key in research, both for the visibility and vetting of research, and for the connections made between researchers that allow synergy, create research partnerships, and create combinatorial improvements.
2. **Reduced funding for cybersecurity research**: NSF will support less research in the field, leading to fewer innovations in cybersecurity. NSF has been a significant supporter of cybersecurity research in the U.S., funding approximately 25% of federally backed basic research at numerous institutions. The anticipated budget cuts, potentially reducing NSF's annual budget from about $9 billion to between $3-4 billion, threaten to significantly diminish the agency's capacity to fund critical research, including research in cybersecurity. This reduction would lead to a decrease in groundbreaking cybersecurity projects and innovations.
3. **Loss of expertise and talent**: The firings at NSF have resulted in the departure of numerous program managers and experts who played crucial roles in evaluating and guiding research proposals. This loss of experienced personnel will hinder the effective allocation of remaining funds and disrupt ongoing cybersecurity research initiatives.
4. **Decline in research opportunities:** With fewer grants available, emerging cybersecurity researchers will find it challenging to secure funding, potentially leading to a talent drain as professionals seek opportunities elsewhere, possibly outside the U.S. This will lead to increases in foreign-funded research, eroding America's lead in the field of cybersecurity innovation. This will also reduce the skill level of the US cybersecurity workforce; lack of cybersecurity skills will significantly impact our ability as a nation to protect our industries, infrastructure and people when adversaries, both foreign and domestic, are on the rise significantly. It is not time to pull back, but to step forward in growing critical cybersecurity skills.
5. **Outdated technology:** As NSF grants typically cover equipment and technology upgrades, universities and labs will struggle with outdated technology, accelerating the decline of US academic institutions and their ability to do cutting-edge research compared to international counterparts.