SDN Security Challenges & Opportunities

Anita Nikolich
National Science Foundation
Program Director, Advanced Cyberinfrastructure

June 2016

Agenda

- NSF-funded SDN research
- NSF-funded SDN implementations
- SDN Workshops and Emerging Themes
- SDN Barriers to Adoption
- SDN Security Research Opportunities
- Other Agencies and SDN
- Ideal Outcome for NSF
- Secure SDN Experimentation
- Funding Opportunities

NSF by the Numbers

$7.72 billion FY 2016 budget request

94% funds research, education and related activities

50,000 proposals

11,000 awards funded

2,000 NSF-funded institutions

300,000 NSF-supported researchers

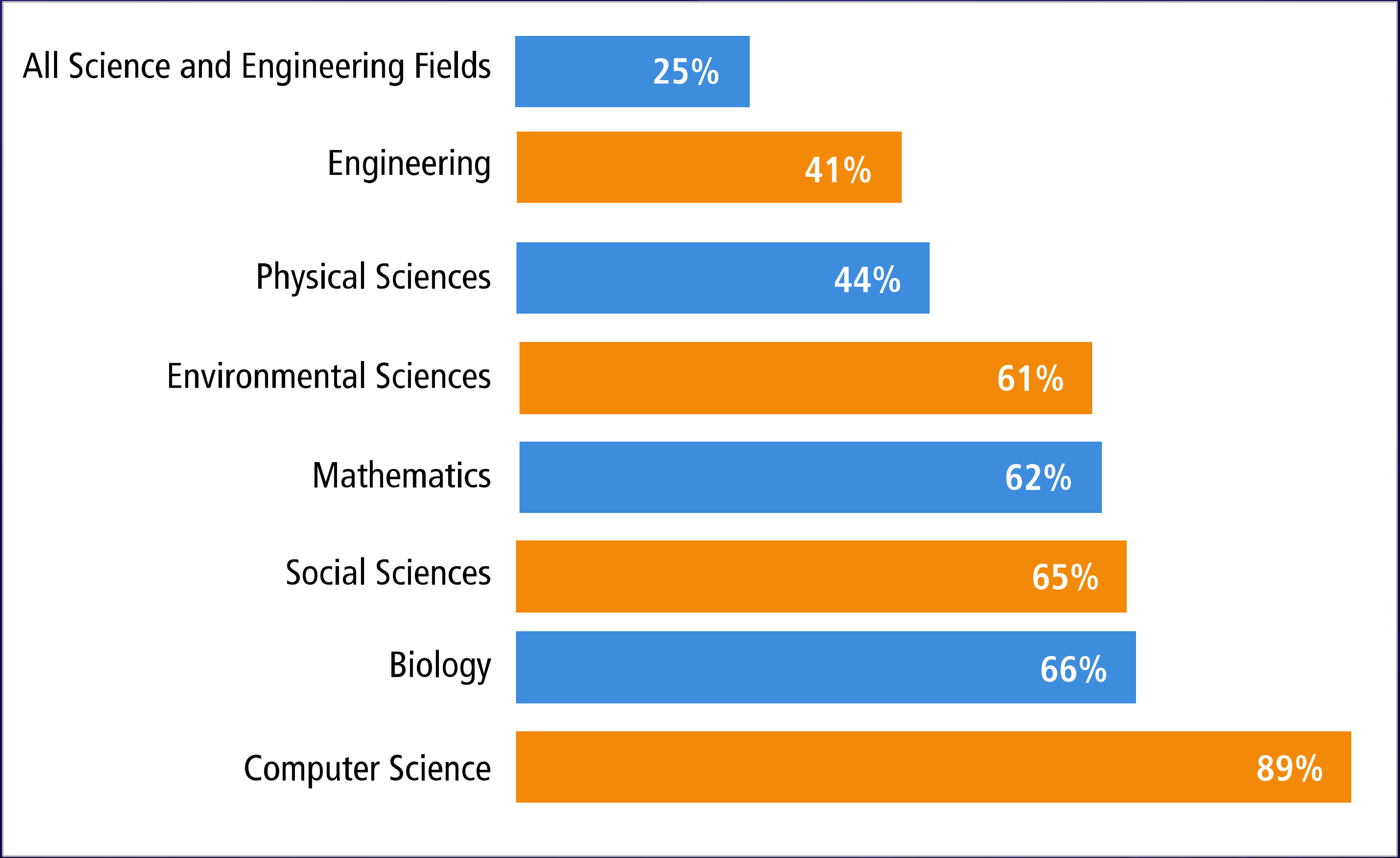
Fund research in all S&E disciplines

Fund STEM education & workforce

217 Nobel Prize winners

NSF Support of Academic Basic Research

(as a percentage of total federal support)



Source: NSF/NCSES, “Survey of Federal Funds for Research& Development, FY 2013. From NSF *FY2016 Budget Request to Congress Request*

Science of Security: Thought Leaders

Carl Landwehr (founded the original NSF SaTC program) – wrote about formal models of security in 1981

Roy Maxion (CMU):

Experimentation

CS students have less training in statistics than social science

Fred Schneider (Cornell) (2012):

"Blueprint for a Science of Cybersecurity":

-transcend specific technologies and attacks, yet still be applicable in real settings

- introduce new models and abstractions

- facilitate discovery of new defenses as well as describe non-obvious connections between attacks, defenses, and policies

Dusko Pavlovic (U Hawaii) (2012):

Security practices lack a method to systematically understand security problems and predict the future behaviors. Need to *invent* a science of security:

- combine various sciences into a new one
- add the experimental method to CS
- measurable validation

Is SDN Security a "Hot Topic"?

- USENIX 2015 HotSec workshop on what makes a hot topic in security
- What role do funding agencies, industry and researchers play in deciding what research to pursue and fund?
- Are there enough basic research questions around SDN Security that NSF should continue funding?

The Bigger Picture: NSF's Funding Source

2011 Federal Cybersecurity R&D Strategic Plan

Coordinated every 5 years by NITRD for the National Science and Technology Council

- 2011 Plan highlighted Science of Security:
  - "…has the potential of producing universal laws that are predictive and transcend specific systems, attacks, and defenses."
  - "…not limited to the traditional, formal mathematical model of reasoning, but extends to experimental science, simulation and data exploration, field studies, social and behavioral science, and principles of engineering."
- Research required to develop:
  - Methods to model adversaries
  - Techniques for component, policy, and system composition
  - A control theory for maintaining security in the presence of partially successful attacks
  - Sound methods for integrating humans in the system: usability and security
  - Quantifiable, forward-looking security metrics (using formal and stochastic modeling methods)
  - Measurement methodologies and testbeds for security properties
  - Comprehensive, open, and anonymized data repositories

Networking and IT Research and Development (NITRD) FY16 Supplement to President's Budget

- Large Scale Networking (LSN):
  - "identify approaches, best practices, and testbed implementations for Software Defined Infrastructure, SDN and SDXs..."
  - "develop, deploy and operate dynamic secure interdomain layers 1, 2 and 3 operational and virtualized networking capability – DoD, DoE, NASA, NIST, NSA, NSF
  - "experimental network facilities"
  - Multiagency workshops: SDN Network planning
- Cybersecurity (CSIA):
  - Accelerating Transition to Practice
  - CyberPhysical Systems (CPS) Security
  - Security for Cloud-based systems

Cybersecurity Enhancement Act 2014

- **Public-Private Collaboration on Security (NIST)**
- **R&D.** "Amends the Cyber Security Research and Development Act to permit NSF R&D grants for: (1) secure fundamental protocols that are integral to inter-network communications and data exchange; (2) secure software engineering and software assurance; (3) holistic system security to address trusted and untrusted components, reduce vulnerabilities proactively, address insider threats, and support privacy; (4) monitoring, detection, mitigation, and rapid recovery methods; and (5) secure wireless networks, mobile devices, and cloud infrastructure."
- **Cybersecurity Testbeds.** "By Dec 2015...NSF... shall conduct a review of cybersecurity test beds, including an assessment of whether a sufficient amount are available. Permits the NSF, if it determines that additional test beds are necessary, to award grants to institutions of higher education or research and development nonprofit institutions to establish such additional test beds."

NSF-funded SDN Research

2011-2015 NSF funded ~60 SDN/NFV proposals or workshops

- NeTS examples:
  - (SDNFV) - Flexible, High Performance Network and Data Center Virtualization
  - Big Data and Optical Lightpaths-Driven Software Defined Networking
  - High-performance Data Plane Kernels for Software Defined Networking
  - A Software Defined Internet Exchange
  - Network Function Virtualization Using Dynamic Reconfiguration

*For a more comprehensive history of SDN, see "The Road to SDN: An Intellectual History of Programmable Networks" (Feamster/Rexford/Zegura)

Secure and Trustworthy Cyberspace (SaTC)

- Cross Directorate Program
- Aims to support fundamental scientific advances and technologies to protect cyber-systems from malicious behavior, while preserving privacy and promoting usability.
- Develop the foundations for engineering systems inherently resistant to malicious cyber disruption
- Cybersecurity is a *multi-dimensional problem*, involving both the strength of security technologies and variability of human behavior.
- Encourage and incentivize socially responsible and safe behavior by individuals and organizations
- Transition to Practice Perspective – encourage later stage research to move into operations or have idea acquired by others to develop

$70M Annually

SaTC FY15-16 Funding Areas

SDN??

SDN??

Access control
Anti-malware
Anticensorship
Applied cryptography
Authentication
Cellphone network security
Citizen science
Cloud security
Cognitive psychology
Competitions
Cryptographic theory
Cyber physical systems
Cybereconomics

Cyberwar
Digital currencies
Education
Forensics
Formal methods
Governance
Hardware security
Healthcare security
Insider threat
Intrusion detection
Mobile security
Network security
Operating systems

Personalization
Privacy
Provenance
Security usability
Situational awareness
Smart Grid
Social networks
Sociology of security
Software security
Vehicle security
Verifiable computation
Voting systems security
Web security

1 award in FY15: “TTP: SRN: On Establishing Secure and Resilient Networking Services (Huang)”

Cybersecurity Innovation for Cyberinfrastructure (CICI) NSF 16-533

Activities that impact the security of science, engineering and education environments

Target community is operational cyberinfrastructure/security

- $7M available. Estimated 7 – 9 awards in 2 Areas (due April 19th):
  - Secure and Resilient Architecture - $1M awards
  - Regional Cybersecurity Collaboration - $500K awards
- 2015 Awards with SDN:
  - CapNet: Secure Scientific Workloads with Capability Enabled Networks (1547457/UUtah/Burtsev)
  - STREAMS: Secure Transport and Research Architecture for Monitoring Stroke Recovery (1547428/UMass Lowell/Luo)
- 2016 Awards TBD soon

NSF-funded SDN Security EAGERs

EAGER: Early Concept Grants for Exploratory Research

$300K and up to 2 years duration

- SDN WAN Security Testbed (SRI/Porras) – joint with KAIST/S. Korea
- SDN Containment Architecture to Enable Secure Role Based Network in Healthcare (UUtah/Van Der Marwe)
- Economic Policies at SDXs (UMass Amherst/Wolf)
- Central IT Ops Support for Production Open Flow (UWisconsin/Maas)

NSF-funded SDN Implementations in Campus Cyberinfrastructure (CC*)

Later stage research and/or production networks

NSF 16-567 due Aug 23, 2016

Network Integration Area seeks to: ” Transition successful research prototypes in Software Defined Networking (SDN)”

- Campus Cyberinfrastructure (CC*) – 25+ SDN based grants since 2012
  - Developing Applications with Networking Capabilities via End to End SDN (DANCES)
  - Data Intensive E-Science and SDN at NCSU
  - A Software Defined Campus Network for Big Data Sciences
  - Advancing Network Capacity , Efficiency and Security for Wisconsin Big Data Research
  - Software Defined and Privacy Preserving Network Measurement Instrument for Data Driven Science Discovery –UMass Lowell
  - Bridging, Transferring and Analyzing Big Data over 100Gb Campus-Wide SDN
  - International SDXs: Atlantic Wave and Starlight SDX

Workshops!

SDN Workshops 2013-2016

- NITRD “Operationalization of SDNs” - Dec 2013
- Korea/US SDN/NFV for Smart Cities – Aug 2014
- Prototyping and Deploying SDXs – June 2014
- Operationalizing SDN – July 2015
- Research Challenges (co-located with ONUG) – Sept 2015
- Beyond the Internet: Software Defined Infrastructures/SDX’s – Feb 2016

NITRD SDN Program Review (2013)

- Security Findings:
  - Poorly understood relationship between switches and controller. How is trust established? How is authorization and authentication done?
  - How to deal with lack of trust between AS’s
  - How to expose policy without compromising security
  - Scalability
- Recommendations:
  - ‘vigorous and sustained research program should investigate the security implications of multi-domain/multi-layer SDNs”
  - ‘research will benefit from close interactions of security researchers with engineers and operators’

Prototyping SDX Workshop (2014)

- Ideas/Themes:
  - Can we solve the problem of inter-domain path end to end with declarative control. BGP can’t do it!
  - Can SDX owners design a prototype, including: trust/authorization, security, optimization, performance
  - Redefine what peering means
  - Explore new paradigms for inter-domain routing and resource identification/allocation/utilization
  - Understand how SDN/SDX can support specific applications not well served on todays’ internet

Common Workshop Themes

SDN is groundbreaking but someone else should try it first!

SDN lacks inherent security – uh oh! Let's bake it in. *crickets*

Some Barriers to SDN Adoption

- Lexicon/vocabulary when defining an authorization policy - identify the correct language for expressing security policies
- What is an SDX? SDX traffic handling still rudimentary
- Lack of security standards and competing organizations – ONF, ETSI, ITU-T, IRTF
- Unclear integration (or not) with BGP and legacy routing
- Confusing products and roadmap from vendors. What’s really SDN vs an overlay?

SDN Challenges

- Distributed state routing algorithms are holding back development
- Scaling. How to deal with the overwhelming amount of flows?
- Controllers (by and large) remain in the development and design stages and are not suitable for production
- Warring controllers – interoperability issues
- Security must be designed in from the start – retrofitting won't work
- Decoupling policies from physical resources

SDN Security Challenges

- Hypervisor – needs strong VM quarantine and isolation – not just an SDN issue
- How is Privacy enforced or recognized?
- SDN Controller – just a few of the issues:
  - Authorization, authentication & access to controller
  - What policies define who can do what to whom?
  - Define explicit mechanisms by which app-level protocols and services may expose information without compromising security

SDN Security Challenges

- Secure interfaces: right now some level of security is possible with things like OpenFlow (e.g., do TLS), but need to do better to make these interfaces secure (e.g., handing error conditions).
- Resource sharing: the centralized controller needs to effectively be able to decide how to allocate resources. A lot of work had been done here, but nothing is operationally viable.
- Access control: With all the different ways to slice and dice an SDN, need better more operationally viable ways to control who is allowed to do what.

SDN Security Research Goals

- Closer coupling between “security” and “networking” research communities
- Broaden the pool of SDN/NFV researchers
- Partner with operational users to understand current and future needed functions
- Policy conflict resolution
- Ability to do network audit – inventory devices on a network
- Better peering policies
- How to peer BGP and SDN traffic
- Characterizing everything on network
- Leverage SDN to deal with HIPPAA, FERPA, ITAR, PCI

SDN Security Research Goals

- Understand needs and motivations of different target communities: carriers, enterprises, government, science
- SDXs – policy chaining, flow governance
- Protocols for Inter-domain
- Better measurement, management and monitoring than traditional networks
- More prototypes! More production traffic
- Quantifying Operational cost savings
- Ensure good software engineering in any code developed

SDN on the WAN

- Global Traffic Engineering
- Interoperating with legacy transport on the Internet
- Real time identification, classification, and control of flows by user or application at scale, enabling advanced network management in an IoT environment.
- Create a Content Delivery Network (ie to stream video from a location closer to user). For NSF science community it's needed for scientific uses. Carriers and content providers need it to differentiate services.
- IXPs / SDXs need strong isolation between participants - parts of the infrastructure are shared among multiple participants.

Opportunities for Operational Security through SDN

- Policies and Verification: Should be a more mathematical way to represent policies and verify that they are being implemented well as well as meet the desired goals. Examples: Policy Graph Architecture (PGA) work from HP, Veriflow work from Urbana Champaign is another.

- Software implementation verification: How can you detect if the software modules implemented and the logic is true to its intent? This could be considered QA and verification of percentage coverage.

- Analytics: How can real-time analytics of flows in SDN help identify and prevent security issues? Things like CTC which are hard to do with deep packet inspection.

SDN for Improved Network Analytics

Dept of Energy’s ESNet SDN Analytics Engine
(Nick Buraglio, Sr. Engineer)

Traditional IDS/IPS’s can’t keep up! They’re built around traditional points of visibility. SDN changes that.

Take Bro IPS/IDS flow data, cross reference for targeted attacks. Use sFlow data as a tertiary data source from edge switches to gain more granular view when combining with router traffic.

Interdomain SDN Security Challenges

- Large numbers of distinct AS’s
- AS’s lack trust
- SDN’s designed as islands – nothing in protocols is interdomain
- Security architecture must be designed for scalability
- SLA, Economic and policy research topics. Can internal information on SDN be shared on a limited basis with peer SDNs and globally connected SDNs
- QoS and resiliency
- Operating in conjunction with BGP and legacy equipment. SDN more than likely will not be greenfield adoption.

Creative Uses of SDN

- Coordinate responses for DDoS mitigation
- Wireless or Cellular
- IoT – more processing at the “edge”, more flexible reconfiguration of devices or removal of insecure devices. Can Security and admission control be done at the edge before it gets into the network?
- Life/Safety - need for near real-time, response, especially for applications involving safety (such as hazardous industrial processes) or commerce (such as monitoring of inventory or customer behavior).
- Security “middlebox” functions
- SDX could be used for compute, storage and networking resource sharing

SDN for Science

- Each science domain has problems that might better be solved using SDN or SDX:
  - Astronomy – radio astronomy uses real time data flows needing high performance streams. LSST
  - Climate Science – moves large amounts of data to local facilities
  - Genomics – already uses SDN-enhanced data transport among multiple campuses
  - Physics – much more LHC data. Estimated 100 PB/mo by mid 2016. Could individual flows be programmed? Could an SDX contain data caches?

Need: SDN-driven flow steering, load balancing, site orchestration over Terabit/sec global networks

Socializing SDN in Network and Security Communities

- Governance model, in particular at the IXPs. How to govern flows and deal with competing traffic? Need mechanism for resolving conflicts.
- New trust model. BGP’s is broken. How can SDN be created better from day one?
- Find users who have a problem to solve. SDN might be best solution. Try a small prototype!

SDN in CyberPhysical Systems (CPS)

Sample areas of interest with secure SDN potential:

- IoT Security
- Smart Manufacturing
- Smart Cities
- Smart and Connected Health
- Secure Vehicles

Other Agencies and SDN Security

Dept of Energy (DoE)/Energy Sciences Network (ESNet)

Connects scientists globally across 100Gb network

Example: Large Hadron Collider (LHC) experiment

- Looking at SDN for future network in support of Exascale computing
- Security architecture for control plane is a requirement!
- Taking a systems perspective - SDN control plane will have multiple controllers, will require authenticated, secure multi-domain conversations between controllers

Other Agencies and SDN Security

NIST

- Emerging program looking at robustness and security issues in SDN/NFV and the standards and measurement science necessary to advance the state of the industry.
- Outputs might include: standards profiles and test programs to protect USG early investments these technologies; security and deployment guidance for their use; novel applications of SDN to address other issues in network security and robustness.

Other Agencies and SDN Security

Department of Homeland Security (DHS) S&T Priorities:

- Security of SDN itself. As new features are added, need to make sure they are added with security in mind.
- New features from SDN may help solve existing security problems that have been very difficult to handle.
  - DDoS attacks have not been solved. DHS is currently funding several efforts that use SDN to defend against DDoSD attacks.
    - USC/ISI and Oregon with subcontract to UCLA
    - Colorado State with subs to UC Riverside and NoFutz Networks.

Refer to DHS S&T:

- Project on Secure Protocols
- DDoSDefense

Testing SDN Security

- Must be done at scale, not via simulation, especially for WAN implementations - Go beyond Mininet
- Australian Research Network (AARNET) has a wide area SDN testbed that connects internationally.
  - 4 Noviflow OF switches running ONOS. Connects to Seattle to Internet2/ESNet to connect to other testbeds.
  - AARNET has SDN between them, New Zealand, South Africa and US.
- ESNet and Internet2 testbeds
- New Zealand – FAUCET controller has added functionality to to some layer 2 type attacks
- Phil Porras (SRI) and KAIST – WAN Testbed
- Partner with those who run SDX's now in the R&E Community – Atlantic Wave & Starlight
- PenTest/Red team attacks on SDN infrastructure
- POSEIDON – automated SDN PenTest framework (KAIST)

Cybersecurity Experimentation of the Future (CEF) Study - 2014

- Engaged the cybersecurity research and CI communities on the needs, requirements, and potential gaps in cybersecurity experimental facilities and capabilities
- Strategic roadmap for developing sustainable infrastructure that supports tomorrow's cybersecurity research
- Experimentation is about learning
  - To perform an evaluation (not formal T&E)
  - To explore a hypothesis
  - To characterize complex behavior
  - To complement a theory
  - To understand a threat
  - To probe and understand a technology

Collaborative effort by SRI International and USC-ISI

CEF: Overall Recommendations for Transformational Progress

Emphasis on infrastructure alone will far fall short of achieving the transformational shift in research, community, and supporting experimentation required

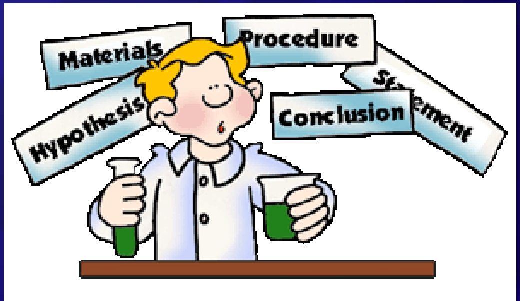
- Fundamental and broad intellectual advance in the field of experimental methodologies and techniques
  - With particular focus on complex systems and human-technical interactions
- New approaches to rapid and effective sharing of data and knowledge and information synthesis
  - That accelerate multi-discipline and cross-organizational knowledge generation and community building
- Advanced experimental infrastructure capabilities and accessibility

CEF: More than Just Infrastructure

- Research infrastructure requires meta-research into:
  - Design specification (multi-layered languages and visualization)
  - Abstraction methodologies and techniques
  - Semantic analysis and understanding of experimenter intent
  - Formal methods and a rich approach to modeling to satisfy science objectives

Future Research Infrastructure Needs

- Data – vetted, provenance-oriented real data
- Accessible by all – open source, virtual
- Serve researchers in multiple domains which can benefit from SDN – Cyber Physical, Networking, Security, Manufacturing, etc



SDN Funding Opportunities

- NeTS - due Sept and Nov. Up to $3M/5 years
- CC* - August 23rd. Specifically calls out SDN.
- CICI (16-533) -– due April 19. Up to $1M/3 years. Specifically calls out SDN.
- SaTC – out soon - due Sept and Nov. Up to $3M/5 years.
  - Transition to Practice (TTP) Perspective!
- CPS (16-549) – due June 7. Up to $7M/5 Years
- EAGER – no set deadline. $300K limit/2 years
- REU supplements to existing awards
- Student travel grants
- Workshops

Final Takeaways

- Don’t repeat the mistakes of the past!
- We may be building on principles of GENI, but this isn’t GENI
- Is SDN security a concern? NSF must hear this message from the research community!
- Creativity and innovation always welcome
- Would an EAGER better serve your idea?
- More cooperation between network/security researchers
- More cooperation between research and operations communities
- Take the human out of the loop - identify and remediate network attacks without a SysAdmin
- Help reviewers understand SDN
- Don’t forget REU supplements if you have a grant!

Want to be a reviewer for SDN?
Want to become an NSF Rotator?

Email me!

anikolic@nsf.gov