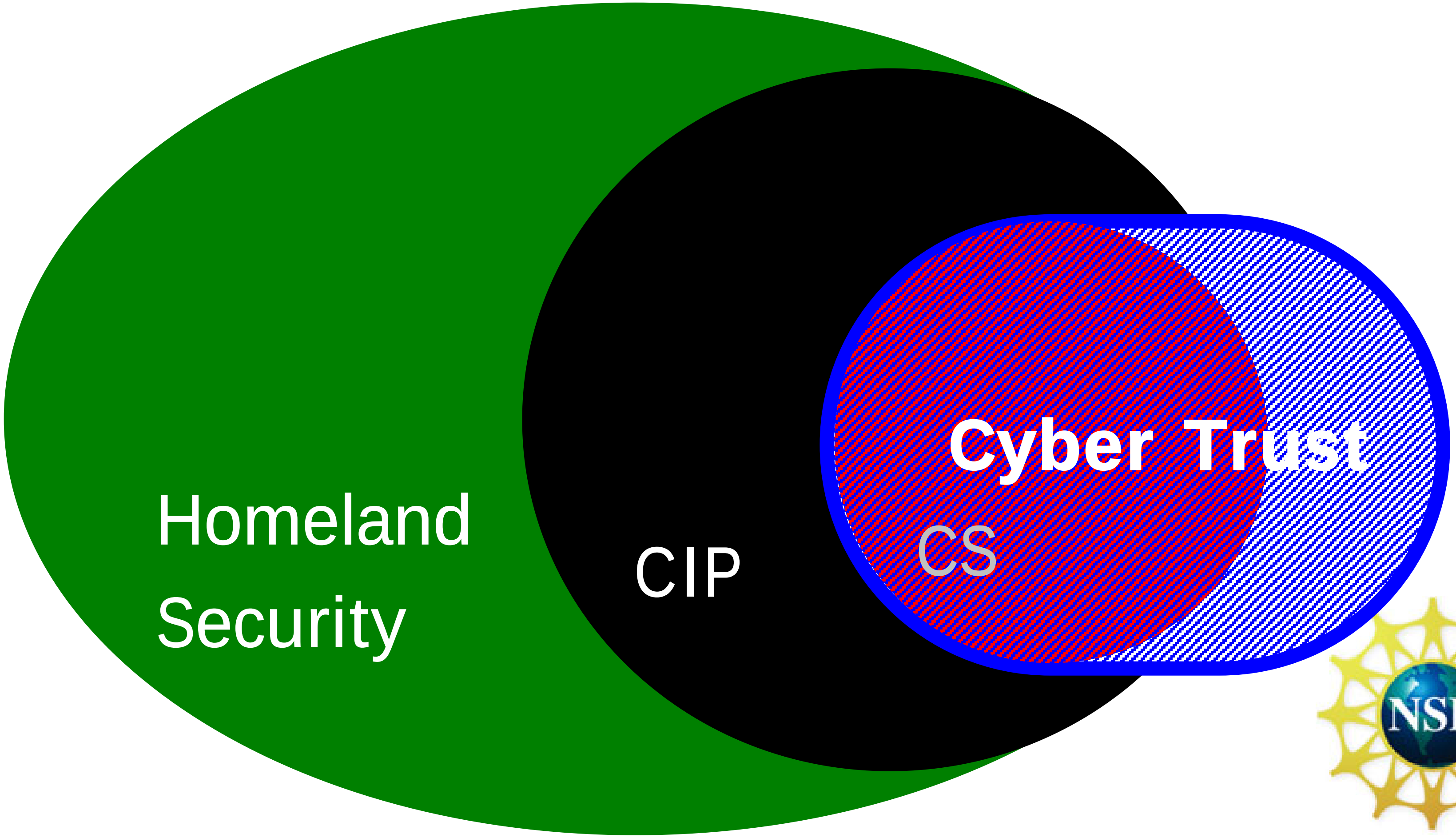
Where Are We Putting Our Research Funds in Cyber Security?

For President's Information Technology Advisory Council

April 13, 2004

Carl Landwehr (clandweh@nsf.gov**)**
Cyber Trust Coordinator
National Science Foundation

Homeland Security
Critical Infrastructure Protection
Cyber Security
Cyber Trust



Cyber Security R&D Act (PL 107-305)

- Recognizes
  - interdependencies of cyber and other infrastructures,
  - lack of preparedness for coordinated physical and cyber attacks,
  - lack of needed research capacity;
- Calls for expanded Federal investment in computer and network security research.
- Authorizes NSF to
  - award grants for **basic** research to enhance cyber security
  - establish research centers for cutting edge, multidisciplinary research
  - build research capacity
  - take a leading role in research and education to improve security of networked information systems
- Also authorizes a variety of activities for NIST

NSF Funding profiles FY04 – FY05[1]

	Research Grants	Research Centers	Capacity Building	Trainee-ships[2]	S. & A. Tech.	Total	Auth.
FY05 (req.)	$36M	$14M	$16M	$8.5M	$1.5M	$76M	$128
FY04	$31M	$10M	$16M	$5.5M	$1.5M	$64M	$110

Caveats:

1. Figures approximate, based on current projections

2. Traineeship numbers reflect graduate students supported through research programs

NSF Cyber Security Investments

Active Research Grants

Broad range of awards addressing cyber security foundations and technologies;

- over 175 active awards
- ITR, NSF Middleware Initiative, Strategic Technologies for Internet, Digital Government, Experimental Infrastructure Networks, and wide range of disciplinary programs contributing
- Special emphasis on Cyber Security topics in new Cyber Trust emphasis, which incorporates
  - Trusted Computing
  - Security-related Network research
  - Data and Application Security
  - Embedded and Hybrid Control Systems

NSF Cyber Security Investments

Active Center Scale Awards

- Large ITR award ($12.5M total):
  - Sensitive Information in a Wired World (Stanford, Yale, Stevens, UNM, NYU): multi-disciplinary investigation of long term issues in automated information handling
- Large scale network testbed established for investigating network attacks, with major support from DHS:
  - Defense Technology Experimental Research (DETER) network, $5.45M total, led by UC-Berkeley, with USC/ISI and others
  - Testing and Benchmarking Methodologies for Future Network Security Mechanisms, to develop attack simulators, traffic generators, datasets for DETER, $5.6M total, (UC-Davis, Penn State, Purdue, ICSI).
- I/UCRCs:
  - Center for Identification Technology Research (Biometrics)(WVU)
  - Cyber Protection Center (Iowa State U, U Kansas, Miss State U)
  - Center for Experimental Research in Computer Systems (Ga Tech)

NSF Cyber Security Investments

Active Capacity Building Grants

- Federal Cyber Service: Scholarship for Service program (EHR)
  - Education:
    - 19 institutions currently supported
  - Capacity Building
    - 19 active grants
  - FY'04 SFS Competition Underway
- Advanced Technological Education (ATE) grants, under Scientific and Advanced Technology Act (S&A T)
  - 7 active awards

Advances and areas of promise

- Things to deal with today’s imperfections
  - Protection against specific attack types (e.g. PointGuard$^{\text{TM}}$)
  - Better static checking of software
    - Bug finding techniques (e.g., RacerX)
    - Model checking for software (and systems?)
- Things for building better systems in the future
  - Improved knowledge about limits (e.g., impossibility of obfuscation)
  - Better understanding of how to apply cryptography for authenticity and privacy in particular applications
  - Language-based security (e.g., PCC, MCC, TAL, inline RMs)
  - Architectures
    - Attestation technology
    - Re-birth of virtual machines
    - Possibility of diverse redundancy
    - Catastrophe-resilient architectures

Other Departments and Agencies Investing in Cyber Security Research

- Defense: DARPA, but also ONR, AFOSR, ARO in various ways, including in-house laboratories
- DHS
- Intelligence Community: NSA, ARDA, In-Q-tel
- Energy
- Commerce: NIST
- DoJ
- FAA

Agency programs typically reflect agency priorities

Balancing NSF's Research Portfolio

- We need to keep our heads up, and we have help
  - research community, government, and industry participate through the peer review process
- Studies can help
  - CSTB Certification study
  - CSTB Cyber Security R&D study
- Workshops can help
  - CRA Grand Challenges workshop
  - DIMACS workshop series
- Coordination can help
  - Infosec Research Council
  - NCO IT R&D WGs
  - CIIP R&D WG

What research areas contribute to improved Cyber Security?

- **System oriented**
  - Architectures for dependability, survivability
  - System management, monitoring, control, measurement
  - Multidisciplinary: human factors, economics, policy
- **Application oriented**
  - Security of applications: web services, e-commerce, database security and privacy, etc.
  - Application level security functions: authentication and authorization mechanisms, policy specification, negotiation, enforcement
- **Infrastructure oriented**
  - Communications: protocols, network security functions, collaboration, accountability, anonymity, forensics
  - Computing: trustworthy OS architectures, access control, secure control
- **Foundational**
  - logic, languages and tools for development of secure systems, composition methods, ways to measure, model, analyze, verify, test

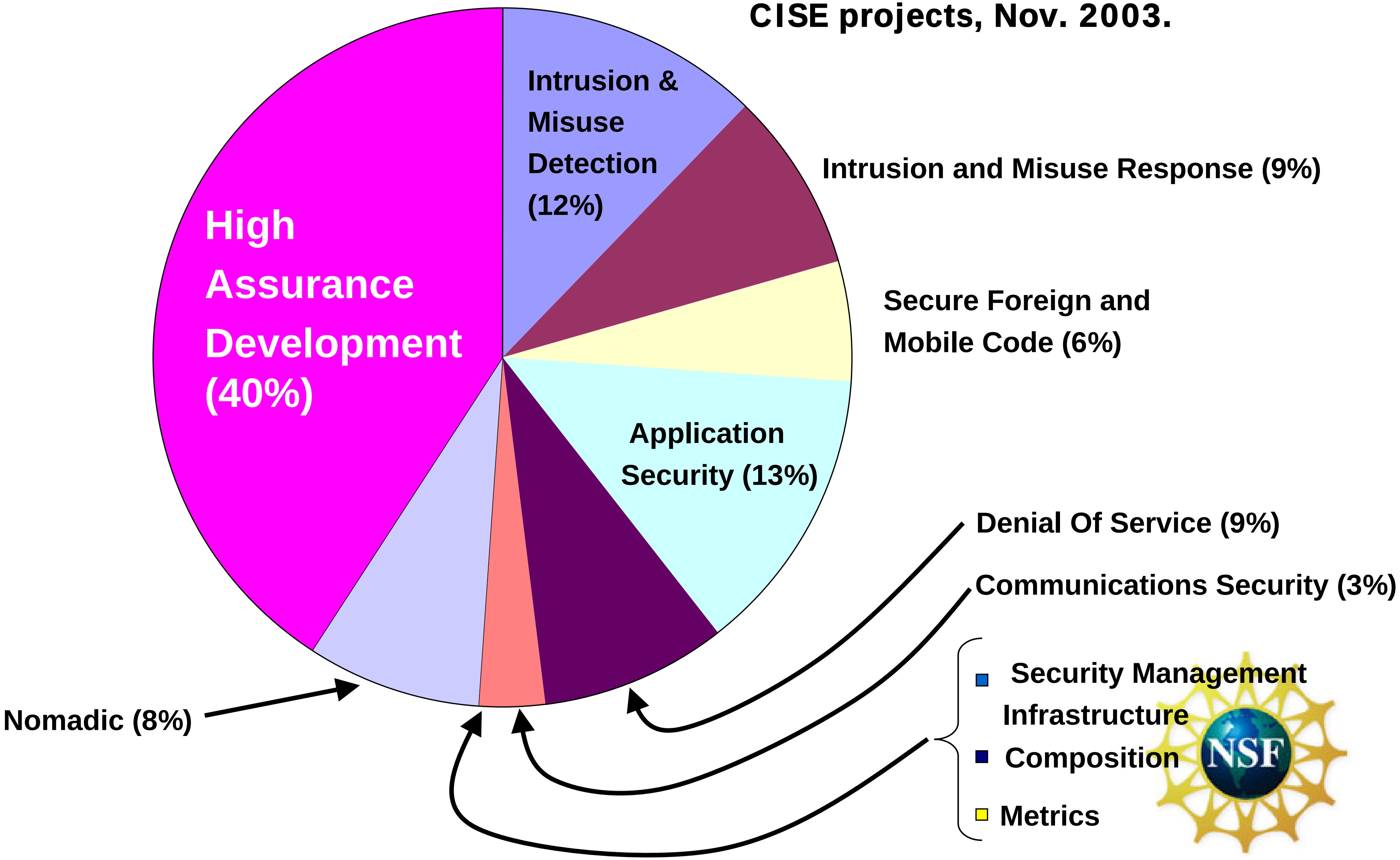
Other ways to view the portfolio

- Assumed context
  - Dealing with the current mess
  - Building a better basis for the future
- DoD (DIAP) strategy: Protect, Defend, IA awareness/control, IA transformation, Building workforce
- IRC hard problem list: 9 functional + 3 development
- CSRDA technology list: 9 broad categories
- CRA IA Grand Challenges: 4 problems

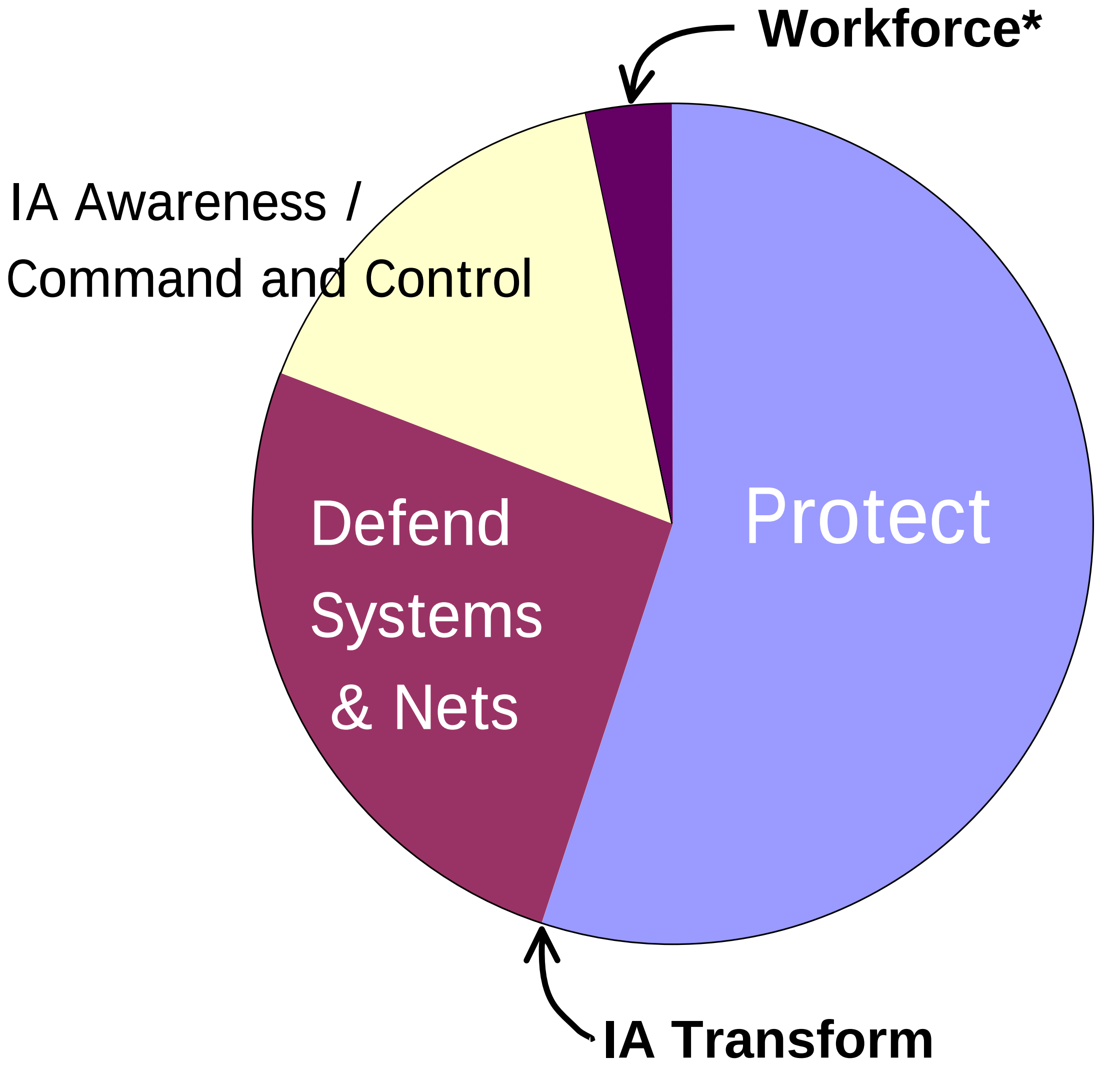
NSF FY ’03 Research Portfolio Balance

By IRC Hard Problem List Categories

Estimated proportion of spending, based on abstracts of a sample of 60 CISE projects, Nov. 2003.



NSF Projects by DoD IA Strategy Goals



* Notes:

1. Nearly all NSF research grants build workforce by training students
2. Scholarships for Service program not included here

Estimated proportion of FY03 spending based on review of ~60/220 CISE project abstracts

Thank you.
Questions?

Carl Landwehr
National Science Foundation
Program Director, Cyber Trust Theme Coordinator
CISE/CNS
E-mail: CLandweh@nsf.gov
703-292-8950