

NSF Cyber Trust Report

For US-Japan CIIP Experts Workshop, Sept 28-29 2004

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

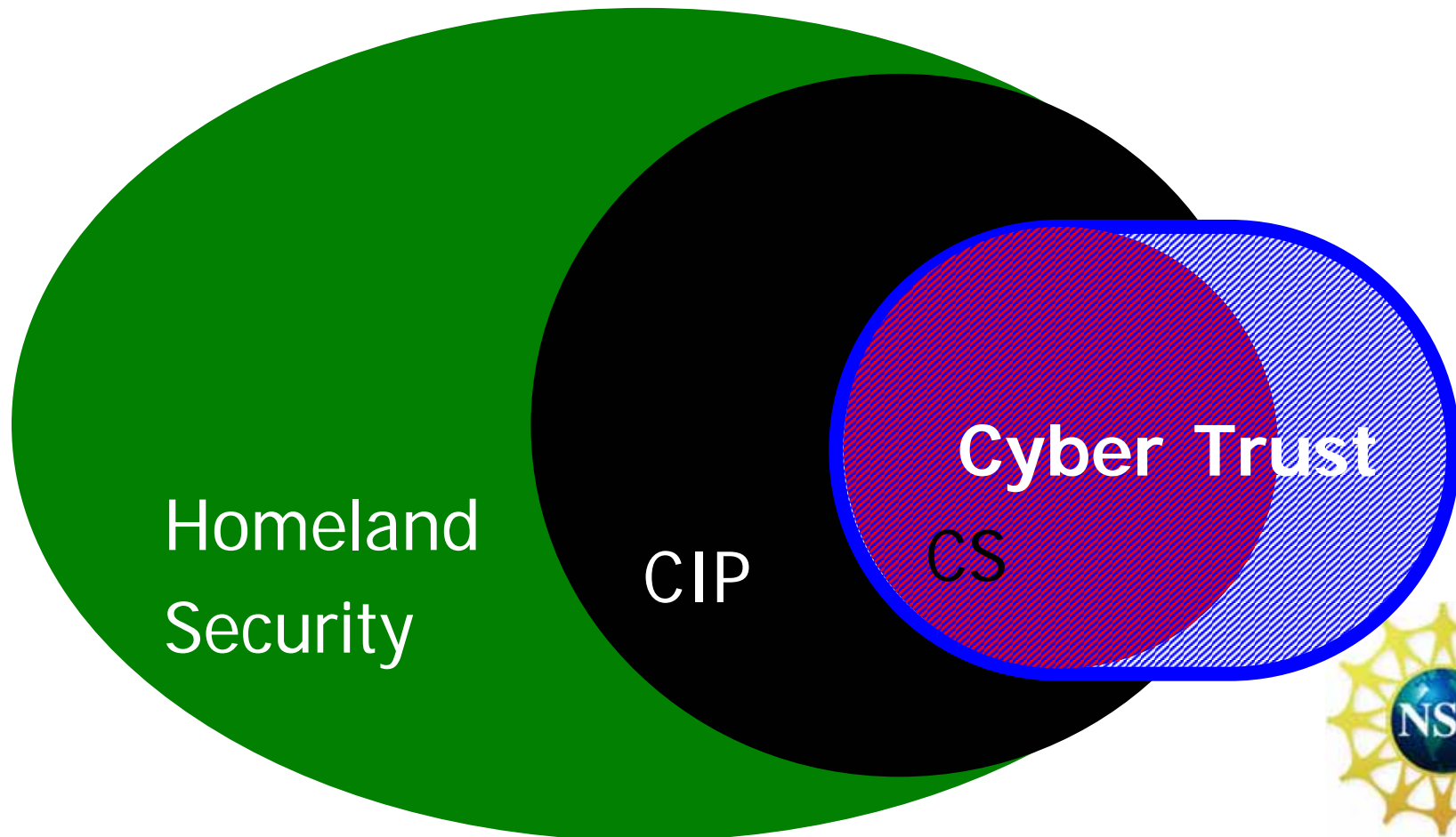


Homeland Security

Critical Infrastructure Protection

Cyber Security

Cyber Trust



Cyber Trust Vision

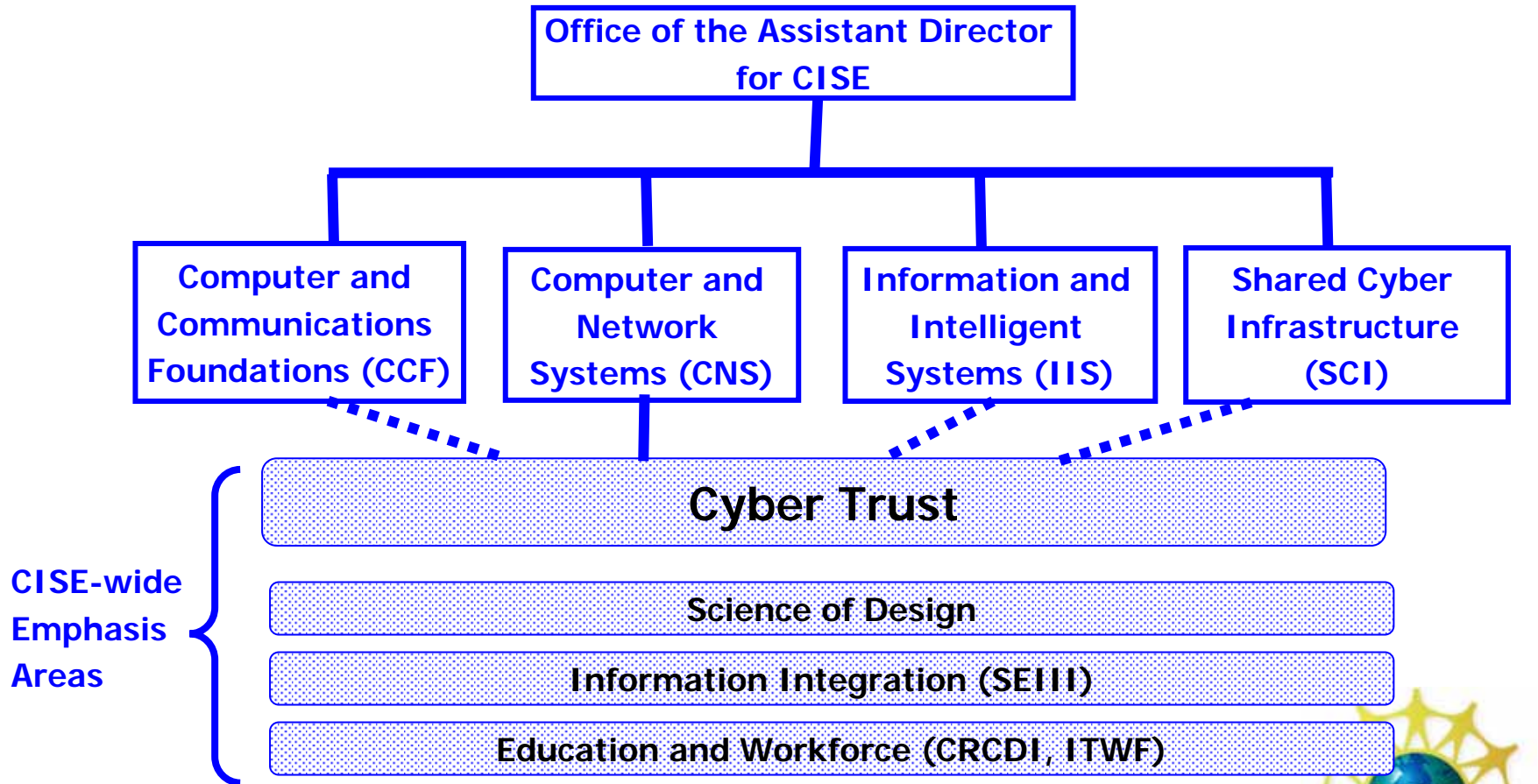
Society in which

- People can justifiably rely on computer-based systems to perform critical functions securely
 - national scale infrastructures: water, power, communication, transportation, ...
 - localized systems: cars, homes, ...
- People can justifiably rely on systems to process and communicate sensitive information securely
 - health, banking, libraries, e-commerce, government records must conform to public policy
- People can rely on a well-trained and diverse workforce to develop, configure, and operate essential computer-based systems

Without fear of sudden disruption by cyber attacks

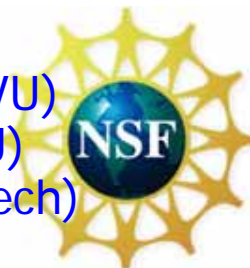


Cyber Trust in CISE



Active Center Scale Awards

- Cyber Trust Center Scale Activity awards
 - CMU: Security through Interaction Modeling (STIM) (\$6.4M, 5 years)
 - UCSD/ICSI: Internet Epidemiology (\$6.2M, 5 years)
- Large ITR award (\$12.5M total, 5 years):
 - 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)



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



Cyber Trust Solicitation FY04

- Released, following substantial internal review, early December, 2003
- 3 categories of proposals
 - Individual / small group: up to \$450K total, due 3 March
 - Team: up to \$2.25M total, due 3 March
 - Center-scale: up to \$10M total, due 31 March
- Limitation: individual can be PI/CoPI/Senior personnel on only two proposals
- Funding fenced among the three categories
- Town hall meeting to inform/attract govt co-sponsors



Response to Cyber Trust Solicitation

- Overall: 489 Proposals
- Individual/small group: 255 proposals, 230 projects
- Team: 189 proposals, 135 projects
- Center Scale: 45 proposals, 25 projects



Proposal Review

- Sixteen panels organized by the CTCG
- Convened panels May – July
- Conferred on results
- Sought co-funding



Award Statistics

- Individual/Small Group: 22 proposals, 18 projects
- Team: 20 proposals, 12 projects
- Center: 3 proposals, 2 projects
- Nearly all awards now public:
 - See NSF awards search page:
 - <http://www-livecds.nsf.gov/awardsearch/tab.do?dispatch=2>
 - select “Program Information” tab
 - Enter in program field: CYBER TRUST



What's next?

- Revised Cyber Trust solicitation planned for release in October
 - Largely similar to last year's content
 - Some tweaks to the submission process
 - Possible name change
- Deadlines expected to be early Feb., 2005
- Resources available – planned for similar level to this year, pending appropriations, as always



Thank you!

