Dated: April 10, 2001.

Madeleine Clayton,

Departmental Paperwork Clearance Officer, Office of the Chief Information Officer.

[FR Doc. 01–9190 Filed 4–12–01; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No. 010323078–1078–01]

RIN 0693–ZA–44

Critical Infrastructure Protection Grants Program

AGENCY: National Institute of Standards and Technology, Commerce.

ACTION: Notice of availability of funds.

SUMMARY: The National Institute of Standards and Technology (NIST) invites proposals from eligible organizations for funding projects under the Critical Infrastructure Protection Grants Program (CIPGP). The objective of the CIPGP is improvement of the robustness, resilience, and security of information in all the critical infrastructures. This will be accomplished by funding research leading to commercial solutions to those information technology (IT) security problems central to critical infrastructure protection that are not being adequately addressed. A secondary objective of the CIPGP is to cultivate a security-capable and security-conscious community. The issuance of all awards under this program is subject to the availability of funds.

DATES: Proposals must be received by 4:00 p.m. Eastern Daylight Time, June 15, 2001.

ADDRESSES: Applicants are requested to submit one signed original and two copies of the proposal to: Kim Morgan; National Institute of Standards and Technology; 100 Bureau Drive, Stop 8901; NIST North, Room 622; Gaithersburg, MD 20899–8901; Tel. (301) 975–3660. Electronic submissions are not acceptable. Questions may be directed to: E-Mail: *kimberly.morgan@nist.gov.*

FOR FURTHER INFORMATION CONTACT: Donald G. Marks; National Institute of Standards and Technology; 100 Bureau Drive, Stop 8930; NIST North, Room 682; Gaithersburg, MD 20899–8930; Tel. (301) 975–5342; E-Mail: *CIP@nist.gov.*

Additional information will be available on the web site, *http://csrc.nist.gov/grants.* Questions regarding administrative matters such as payments or required forms should be directed to the NIST Grants Office at (301) 975–5718.

SUPPLEMENTARY INFORMATION:

Authority: 15 U.S.C. 278g–3 and 15 U.S.C. 272(b) and (c).

Background

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include telecommunications, energy, banking and finance, transportation, water systems and emergency services. Many government agencies rely upon these commercially-provided systems to deliver essential government services. The importance of these systems is not lost upon those with interests inimical to those of the United States. Indeed, the fact that these systems are critical makes them targets.

Due to advances in information technology (IT) and the necessity of improved efficiency, these infrastructures have become increasingly automated and interdependent. Most modern commercial infrastructures are composed of a collection of interconnected networks that serve different purposes and have different owners. Critical information is passed between these component networks to coordinate necessary functions. The complexity and interdependency of this critical information flow introduces vulnerabilities into the entire critical infrastructure. These vulnerabilities may lead to deliberate attacks or accidental system failure, resulting in serious consequences to the nation.

In order to provide satisfactory infrastructure security, additional research must be conducted on the unique infrastructure security problems. While the United States Government has sponsored considerable research in the area of computer security for military and intelligence systems, there has been insufficient research to address the protection of private, commercial, and civil infrastructures. The new CIPGP, administered by the National Institute of Standards and Technology (NIST), recognizes that significant additional research is needed to target infrastructure IT security issues applicable to civilian and commercial systems.

Program Description and Objectives

The objective of the CIPGP is improvement of the robustness, resilience, and security of information in all the critical infrastructures. At first glance, many of the research areas that apply to traditional information security also seems to apply to critical infrastructure security. however, infrastructure systems tend to be larger, more complex and heterogeneous than typical computer-based information networks. Proposals must be properly targeted at infrastructure issues. Proposed research should investigate innovative approaches and techniques that lead to or enable significant advances in the state-of-the-art of IT security applicable to commercial and civilian critical infrastructures. Research should result in proof-of-concept hardware and/or software demonstrating integrated concepts and approaches that apply to large-scale real or virtual networks. Integrated solution sets embodying significant technological advances are strongly encouraged over narrowly defined research endeavors. Proposals should clearly explain what commercial or government entities are likely to utilize the solution and how this proposal contributes to that utilization. Applicants must have a proactive ''technology transition'' plan to facilitate the necessary technology transfer to the appropriate organizations. We encourage proposals involving cooperation among multiple parties, including academic and commercial groups.

A number of key research areas are likely to be involved with the successful development of CIP solutions. The CIPGP is generally interested in the areas of:

Threat/Vulnerability/Risk Assessments. As its name implies, this area focuses on threat, vulnerability, and risk assessments of all critical infrastructures, but especially those with under-analyzed or unique technologies. The area also includes interdependency considerations, modeling and simulation programs, metrics, and testbeds.

System Protection. This area covers cyber protection of individual, interlinked, or interdependent systems. It includes issues such as design and composibility of secure large-scale systems, encryption, public key infrastructures, network security products, reliability and security of computing systems, information access controls, and robust IT controls for power grids.

Intrusion Monitoring and Response. This area examines technologies to accurately detect and swiftly respond to intrusions or infrastructure attacks, including network intrusion detection, information assurance technologies, mobile code and agents, network alarm systems, forensic tools for electronic

media, and network defensive technologies.

Reconstitution. This area concentrates on those technologies required to reconstitute and restore critical infrastructures in the aftermath of disruptions. Specific research areas include risk management studies and tools, disaster recovery, system survivability technologies, interdependence and consequence analysis tools and supporting technologies.

Rather than focus the research on a limited set of issues, the CIPGP is seeking the very best innovative ideas from the community. As a result, it is necessary that all applicants explain why the research is applicable to a CIP problem, justify the importance of the particular problem being addressed, establish that current research is inadequate to solve the problem, explain the impact of the research, and present a plan to utilize the results.

For FY 2001, emphasis will be placed on the following topics as identified by the President's Committee of Advisors on Science and Technology (the PCAST):

- Network system interactions and vulnerabilities to cascading effects;
- Robustness, resilience, and behavior of tightly coupled, complex, nonlinear systems;
- Design of ''testbeds'' and other means for experimentally validating network security technologies;
- Fundamental principles, scientific basis, methodologies, and metrics for information assurance as an engineering discipline;
- Information assurance for emerging information technologies;
- Concepts for high-confidence systems and software;
- Increasing resistance to penetration;
- Next-generation intrusion and malicious code detection;
- User interfaces such as visualization of system security information;
- Self-healing systems;
- Security and forensics toolkits; and
- System architecture to ensure survivability, graceful degradation under stress, and ease of reconstitution.

Eligibility

Eligible applicants are institutions of higher education, other nonprofits, commercial organizations, foreign organizations and governments, international organizations, and state, local, and Indian tribal governments.

Research projects involving cooperation of multiple parties, such as universities and private businesses, are strongly encouraged. Proposals involving cooperation among multiple parties should be submitted by a single applicant, with a description of the proposed arrangements with other parties (through subcontracts and subawards) included in the project description and budget. When such a proposal is selected for funding, NIST will issue the funding directly to the applicant, who is responsible for complying with arrangements with contractors and subrecipients.

Funding Availability

In fiscal year 2001, the CIPGP anticipates funding of approximately $4,500,000. Typical awards are expected to range from approximately $100,000 to $1,000,000 over a two year period, although proposals up to $1,500,000 will be considered, and proposals for small grants (any grant or cooperative agreement not exceeding the small purchase threshold, currently at $100,000) are encouraged. Awards are contingent on the availability of funds.

Proposal Review and Evaluation Criteria

Proposals will be reviewed in a three-step process. First, at least three independent, objective individuals knowledgeable about the particular scientific area described in the section above that the proposal addresses will separately conduct a technical review of each proposal, based on the evaluation criteria described below. Second, the Division Chief will make application selections. In making application selections, the Division Chief will take into consideration the evaluation of each technical reviewer; the evaluation criteria listed below; the variety of the proposed activities; the availability of funds; and the degree to which the slate of applications, taken as a whole, satisfies the program's stated purposes. Any deviation from the ranking based on the technical reviews will be based on these factors and will be justified in writing. The final approval of selected applications and award of financial assistance will be made by the NIST Grants Officer based on compliance with application requirements as published in this notice, compliance with applicable legal and regulatory requirements, and whether the recommended applicants appear to be responsible. Applicants may be asked to modify objectives, work plans, or budgets and provide supplemental information required by the agency prior to award. The decisions of the Grants Officer are final. Technical evaluation criteria are:

a. Technical Quality of the Research

The independent reviewers (reviewers) will assess the technical quality based upon:

- Importance of the problem;
- Innovative claims for the proposed research;
- Comparison with other research efforts;
- Tangible benefits to end users;
- Critical technical barriers;
- The proposed approach to overcome the technical barriers; and
- Confidence that the proposed approach will overcome the technical barriers.

The reviewers will also consider how the proposal fits to the objectives described in the Program Objectives section of this notice. (0–50 points).

b. Potential Impact of the Results

Reviewers will assess the potential impact on commercial CIP systems. Consideration will be given to the likely costs and benefits of the solution on future commercial systems, the technical and business obstacles to acceptance, and the quality of the tech transfer plan to address these issues. (0–25 points).

c. Quality of Personnel and Facilities

Reviewers will evaluate the quality of the facilities and experience of the staff, including key personnel who are assigned a significant role in the project, to assess the likelihood of achieving the objective of the proposal. (0–15 points).

d. Cost and Budget Realism

Reviewers will assess the budget against the proposed work to ascertain the reasonableness of the request. (0–10 points)

Award Period

Proposals will be considered for research projects from one to four years. If a proposal for a multi-year project is approved, generally funding for the project is provided in annual increments subject to the availability of funding, satisfactory progress, and continued relevance to the CIPGP mission. Amendment of any award to continue funding or extend an award beyond the originally funded period of performance is at the total discretion of NIST. Multi-year projects must have scopes of work that can easily be separated into annual increments of meaningful work that represents solid accomplishments if continued funding is not made available to the applicant.

Matching Requirements

The CIPGP does not require any matching funds.

Catalog of Federal Domestic Assistance Name and Number: Measurement and Engineering Research and Standards—11.609.

Application Kit

An application kit, containing all required application forms and certifications is available by contacting Ms. Kim Morgan, (301) 975–3660. The application kit is also available at the web site, *http://csrc.nist.gov/grants*, although there is no guarantee of compatibility or interoperability with any specific applicant's hardware or software. All forms must be filled out and included as printed copies with the submission. Electronic submissions are not acceptable.

The application kit includes the following: (Although there is no required format, all forms and the proposal must be clear and easy to read—12 point font or larger recommended wherever possible.)

• SF 424 (Rev 7/97)—*Application for Federal Assistance and Proposal* (no more than 25 pages).

• SF 424A (Rev 7/97)—*Budget Information Non-Construction Programs,* including a detailed budget narrative explaining the details of each budget category and the basis for the cost. Proposals must include costs for two trips to NIST for technical exchange meetings. If indirect costs are included in the budget, a copy of the applicant's negotiated indirect cost rate must be submitted, if available. Commercial organization applicants that do not generally have an independent audit of their financial statements should include an amount in the budget to cover the cost of such an audit. An organizational or project specific audit will be a condition of any award in response to this announcement.

• SF 424B (Rev 7/97)—*Assurances—Non-Construction Programs.*

• CD 511 (7/91)—*Certification Regarding Debarment, Suspension, and Other Responsibility Matters; Drug-Free Workplace Requirements and Lobbying.*

• CD 512 (7/91)—*Certification Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion—Lower Tier Covered Transactions and Lobbying.*

• SF–LLL—*Disclosure of Lobbying Activities.*

• CD–346—*Applicant for Funding Assistance.*

Paperwork Reduction Act

The Standard Forms 424, 424A, 424B and SF–LLL in the application kit are subject to the requirements of the Paperwork Reduction Act and have been approved by the Office of Management and Budget (OMB) under Control Number 0348–0043, 0348–0044, 0348–0040, and 0348–0046, respectively. CD–346 is approved under OMB Control Number 0605–0001.

Notwithstanding any other provision of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with a collection, subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

Research Projects Involving Human Subjects, Human Tissue, Data or Recordings Involving Human Subjects

Any proposal that includes research involving human subjects, human tissue, data or recordings involving human subjects must meet the requirements of the Common Rule for the Protection of Human Subjects, codified for the Department of Commerce at 15 CFR Part 27. In addition, any proposal that includes research on these topics must be in compliance with any statutory requirements imposed upon NIH and other federal agencies regarding these topics, all regulatory policies and guidance adopted by NIH, FDA, and other federal agencies on these topics, and all Presidential statements of policy on these topics.

On December 3, 2000, the U.S. Department of Health and Human Services (DHHS) introduced a new Federalwide Assurance of Protection of Human Subjects (FWA). The FWA covers all of an institution's Federally-supported human subjects research, and eliminates the need for other types of Assurance documents. In anticipation of the new FWA, the Office for Human Research Protections (OHRP), DHHS, has suspended processing of multiple project assurance (MPA) renewals. All existing MPAs will remain in force until further notice. OHRP will continue to accept new single project assurances (SPAs) until approximately March 1, 2001. For information about FWAs, please see the OHRP website at *http://ohrp.osophs.dhhs.gov/whatsnew.htm.*

In accordance with the OHRP, DHHS change, NIST will continue to accept the submission of human subjects protocols that have been approved by Institutional Review Boards (IRBs) possessing a current, valid MPA from DHHS. NIST also will accept the submission of human subjects protocols that have been approved by IRBs possessing a current, valid FWA from DHHS. NIST will not issue an SPA for any IRB reviewing any human subjects protocol proposed to NIST.

Research Projects Involving Vertebrate Animals

Any proposal that includes research involving vertebrate animals must be in compliance with the National Research Council's Guide for the Care and Use of Laboratory Animals which can be obtained from National Academy Press, 2101 Constitution Avenue, NW., Washington, DC 20055. In addition, such proposals must meet the requirements of the Animal Welfare Act (7 U.S.C. 2131 et seq.), 9 CFR Parts 1, 2, and 3, and if appropriate, 21 CFR Part 58. These regulations do not apply to proposed research using pre-existing images of animals or to research plans that do not include live animals that are being cared for, euthanased, or used by the project participants to accomplish research goals, teaching, or testing. These regulations also do not apply to obtaining animal materials from commercial processors of animal products or to animal cell lines or tissues from tissue banks.

Type of Funding Instrument

Proposals selected for funding will be funded through a grant or cooperative agreement, depending on the nature of the proposed work. A grant will be used unless NIST is substantially involved in the project, in which case a cooperative agreement will be used. A common example of substantial involvement is collaboration between NIST scientists and recipient scientists or technicians. Further examples are listed in Section 5.03.d of Department of Commerce Administrative Order 203–26, which can be found at http://www.osec.doc.gov/bmi/daos/203–26.htm. NIST will make decisions regarding the use of a cooperative agreement on a case-by-case basis. Funding for contractual arrangements for services and products for delivery to NIST is not available under this announcement.

Additional Requirements

Primary Application Certifications

All primary applicant institutions must submit a completed form CD–511, ''Certifications Regarding Debarment, Suspension and Other Responsibility Matters; Drug-Free Workplace Requirements and Lobbying,'' and the following explanations must be provided:

1. *Nonprocurement Debarment and Suspension.* Prospective participants (as defined at 15 CFR Part 26, Section 105) are subject to 15 CFR Part 26, ''Nonprocurement Debarment and Suspension'' and the related section of

the certification form prescribed above applies;

2. *Drug-Free Workplace.* Grantees (as defined at 15 CFR Part 26, Section 605) are subject to 15 CFR Part 26, Subpart F, ''Government wide Requirements for Drug-Free Workplace (Grants)'' and the related section of the certification form prescribed above applies;

3. *Anti-Lobbying.* Persons (as defined at 15 CFR Part 28, Section 105) are subject to the lobbying provisions of 31 U.S.C. 1352, ''Limitation on use of appropriated funds to influence certain Federal contracting and financial transactions,'' and the lobbying section of the certification form prescribed above applies to applications/bids for grants, cooperative agreements, and contracts for more than $100,000, and loans and loan guarantees for more than $150,000, or the single family maximum mortgage limit for affected programs, whichever is greater.

4. *Anti-Lobbying Disclosure.* Any applicant institution that has paid or will pay for lobbying using any funds must submit an SF–LLL, ''Disclosure of Lobbying Activities,'' as required under 15 CFR part 28, Appendix B.

5. *Lower-Tier Certifications.* Recipients shall require applicant/bidder institutions for subgrants, contracts, subcontracts, or other lower tier covered transactions at any tier under the award to submit, if applicable, a completed form CD–512, ''Certifications Regarding Debarment, Suspension, Ineligibility and Voluntary Exclusion—Lower Tier Covered Transactions and Lobbying'' and disclosure form, SF–LLL, ''Disclosure of Lobbying Activities,'' Form CD–512 is intended for the use of recipients and should not be transmitted to NIST. SF–LLL submitted by any tier recipient or subrecipient should be submitted to NIST in accordance with the instructions contained in the award document.

Name Check Reviews

All for-profit and non-profit applicants will be subject to a name check review process. Name checks are intended to reveal if any key individuals associated with the applicant have been convicted of or are presently facing, criminal charges such as fraud, theft, perjury, or other matters which significantly reflect on the applicant's management honesty or financial integrity. Form CD–346 must be completed for all personnel with key programmatic or fiduciary responsibilities.

Preaward Activities

Applicants (or their institutions) who incur any costs prior to an award being made do so solely at their own risk of not being reimbursed by the Government. Notwithstanding any verbal assurance that may have been provided, there is no obligation on the part of NIST to cover pre-award costs.

No Obligation for Future Funding

If an application is accepted for funding, DOC has no obligation to provide any additional future funding in connection with that award. Renewal of an award to increase funding or extend the period of performance is at the total discretion of NIST.

Past Performance

Unsatisfactory performance under prior Federal awards may result in an application not being considered for funding.

False Statements

A false statement on an application is grounds for denial or termination of funds, and grounds for possible punishment by a fine or imprisonment as provided in 18 U.S.C. 1001.

Delinquent Federal Debts

No award of Federal funds shall be made to an applicant who has an outstanding delinquent Federal debt until either:

1. The delinquent account is paid in full,

2. A negotiated repayment schedule is established and at least one payment is received, or

3. Other arrangements satisfactory to DoC are made.

Indirect Costs

Regardless of any approved indirect cost rate applicable to the award, the maximum dollar amount of allocable indirect costs for which the DoC will reimburse the Recipient shall be the lesser of:

(a) the Federal Share of the total allocable indirect costs of the award based on the negotiated rate with the cognizant Federal agency as established by audit or negotiation; or

(b) the line item amount for the Federal share of indirect costs contained in the approved budget of the award.

Purchase of American-made Equipment and Products

Applicants are hereby notified that they are encouraged, to the greatest practicable extent, to purchase American-made equipment and products with funding provided under this program.

Federal Policies and Procedures

Recipients and subrecipients of the CIPGP shall be subject to all Federal laws and Federal and Departmental regulations, policies, and procedures applicable to financial assistance awards, including 15 CFR Part 14 and 15 CFR Part 24, as applicable.

The CIPGP does not directly affect any state or local government.

Applications under the CIPGP are not subject to Executive Order 12372, ''Intergovernmental Review of Federal Programs.''

Executive Order Statement

This funding notice was determined to be ''not significant'' for purposes of Executive Order 12866.

Dated: April 7, 2001.

Karen H. Brown,

Deputy Director.

[FR Doc. 01–9247 Filed 4–12–01; 8:45 am]

BILLING CODE 3510–13–M

COMMITTEE FOR THE IMPLEMENTATION OF TEXTILE AGREEMENTS

Adjustment of Import Limits for Certain Cotton, Wool and Man-Made Fiber Textile Products Produced or Manufactured in the Philippines

April 9, 2001.

AGENCY: Committee for the Implementation of Textile Agreements (CITA).

ACTION: Issuing a directive to the Commissioner of Customs adjusting limits.

EFFECTIVE DATE: April 13, 2001.

FOR FURTHER INFORMATION CONTACT: Naomi Freeman, International Trade Specialist, Office of Textiles and Apparel, U.S. Department of Commerce, (202) 482–4212. For information on the quota status of these limits, refer to the Quota Status Reports posted on the bulletin boards of each Customs port, call (202) 927–5850, or refer to the U.S. Customs website at http://www.customs.gov. For information on embargoes and quota re-openings, refer to the Office of Textiles and Apparel website at http://otexa.ita.doc.gov.

SUPPLEMENTARY INFORMATION:

Authority: Section 204 of the Agricultural Act of 1956, as amended (7 U.S.C. 1854); Executive Order 11651 of March 3, 1972, as amended.

The current limits for certain categories are being increased for the recrediting of unused carryforward.

A description of the textile and apparel categories in terms of HTS