proposed project be made to the FTZ Board (19 U.S.C. 81b and 81f; 15 CFR 400.24–26) before a license can be issued or a zone can be expanded. The Act and Regulations require that applications contain detailed information on facilities, financing, operational plans, proposed manufacturing operations, need, and economic impact. Manufacturing activity in zones, which is primarily conducted in subzones, can involve issues related to domestic industry and trade policy impact. Such applications must include specific information on the Customs-tariff related savings that result from zone procedures and the economic consequences of permitting such savings. The FTZ Board needs complete and accurate information on the proposed operation and its economic effects because the Act and Regulations authorize the Board to restrict or prohibit operations that are detrimental to the public interest.

II. Method of Collection

U.S. firms or organizations submit applications to the Foreign-Trade Zones Board.

III. Data

OMB Number: 0625–0139.

Form Number: N/A.

Type of Review: Regular Submission.

Affected Public: State, local, or tribal governments or not-for-profit institutions applying for foreign trade zone status, for subzone status, or for modification of existing status.

Estimated Number of Respondents: 100.

Estimated Time Per Response: 20 to 120 hours (depending on type of application).

Estimated Total Annual Burden Hours: 9,314 hours.

Estimated Total Annual Costs: The estimated annual cost for this collection is $1,043,690.00 ($328,670.00 for respondents and $715,020.00 for federal government).

IV. Request for Comments

Comments are invited on (a) whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden (including hours and costs) of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or forms of information technology.

Comments submitted in response to this notice will be summarized and/or included in the request for OMB approval of this information collection; they also will become a matter of public record.

Dated: April 10, 2001.

Madeleine Clayton,

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

[FR Doc. 01–9189 Filed 4–12–01; 8:45 am]

BILLING CODE 3510–DS–P

DEPARTMENT OF COMMERCE

International Trade Administration

Annual Report for Foreign Trade Zones; Proposed collection; comment request.

SUMMARY: The Department of Commerce, as part of its continuing effort to reduce paperwork and respondent burdens, invites the general public and other Federal agencies to take this opportunity to comment on the continuing information collections, as required by the Paperwork Reduction Act of 1995, Public Law 104–13 (44 U.S.C. 3506(c)(2)(A)).

DATES: Written comments must be submitted on or before June 12, 2001.

ADDRESSES: Direct all written comments to Madeleine Clayton, Departmental Paperwork Clearance Officer, (202) 482–3129, Email *Mclayton@doc.gov.,* Department of Commerce, Room 6086, 14th & Constitution Avenue, NW, Washington, DC 20230.

FOR FURTHER INFORMATION CONTACT: Request for additional information or copies of the information collection instructions should be directed to: Andrew McGilvray, Foreign Trade Zones Staff, Room 4008, 14th & Constitution Avenue, NW, Washington, DC 20230; Phone number: (202) 482–2862, and fax number: (202) 482–0002. The FTZ Annual Report Form and Guidelines, as well as the Regulations, are available on-line at http://ia.ita.doc.gov/ftzpage.

SUPPLEMENTARY INFORMATION:

I. Abstract

The Foreign-Trade Zone Annual Report is the vehicle by which Foreign Trade Zone (FTZ) grantees report annually to the Foreign Trade Zones Board, pursuant to the requirements of the Foreign Trade Zones Act (19 U.S.C. 81a–81u). The annual reports submitted by grantees are the only complete source of compiled information on FTZ's. The data and information contained in the reports relates to international trade activity in FTZ's. The reports are used by the Congress and the Department to determine the economic effect of the FTZ program. The reports are also used by the FTZ Board and other trade policy officials to determine whether zone activity is consistent with U.S. international trade policy, and whether it is in the public interest. The public uses the information regarding activities carried on in FTZ's to evaluate their effect on industry sectors. The information contained in annual reports also helps zone grantees in their marketing efforts.

II. Method of Collection

FTZ grantees submit annual reports to the Foreign-Trade Zones Board.

III. Data

OMB Number: 0625–0109.

Form Number: ITA–359P.

Type of Review: Regular Submission.

Affected Public: State, local, or tribal governments or not-for-profit institutions which are FTZ grantees.

Estimated Number of Respondents: 150.

Estimated Time Per Response: 38 to 211 hours (depending on the size and structure of the FTZ).

Estimated Total Annual Burden Hours: 13,352 hours.

Estimated Total Annual Costs: The estimated annual cost for this collection is $585,507.00 ($509,607.00 for respondents and $75,900.00 for federal government).

IV. Request for Comments

Comments are invited on (a) whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden (including hours and costs) of the proposed collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; and (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or forms of information technology.

Comments submitted in response to this notice will be summarized and/or included in the request for OMB approval of this information collection; they also will become a matter of public record.

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