Westlaw Journal
GOVERNMENT CONTRACT
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 27, ISSUE 7 / AUGUST 5, 2013

Expert Analysis

NIST's Proposed Cybersecurity Research and Development Center

By Dismas N. Locaria, Esq., Andrew Bigart, Esq., and Keir Bancroft, Esq.
Venable

On April 22 the National Institute of Standards and Technology announced plans to sponsor a "federally funded research and development center" to support the agency's National Cybersecurity Center of Excellence. The NCCoE is a public-private collaboration to accelerate the widespread adoption of integrated cybersecurity tools and forms of technology.

An FFRDC is a quasi-governmental research entity that by law must be managed by a not-for-profit entity or an industrial firm. The NIST has announced plans to solicit proposals from private industry to manage the FFRDC later this year.

This commentary provides entities who are interested in proposing to manage the FFRDC with a primer on the program and some issues to bear in mind when pre-positioning to compete for the contract award.

WHAT ARE THE NIST AND THE NCCOE?

The NIST, part of the U.S. Department of Commerce, is a non-regulatory federal agency that promotes U.S. innovation and industrial competitiveness by advancing science, standards and technology in ways that enhance the nation's economic security. In this role, the NIST's Computer Security Division has been a leading voice in the cybersecurity world for many years. Most recently, in President Obama's Feb. 12 executive order "Improving Critical Infrastructure Cybersecurity," the NIST was directed to work with stakeholders to develop a voluntary framework for reducing cyber risks to critical infrastructure.[1]

The NCCoE was established in 2012 by the NIST through a partnership with the state of Maryland and Montgomery County, Md. The NCCoE's focus is to provide private industry with "real-world cybersecurity capabilities based on commercially available technologies." To accomplish this goal, the center works with experts from private industry, the U.S. government and academia to develop cybersecurity solutions.

WHAT IS AN FFRDC?

The genesis for today's FFRDC program can be traced back to the U.S. government's mobilization of the country's public and private scientific and engineering talent during World War II. The first official FFRDC (then called a federal contract research

center) was RAND, which was created by the U.S. Air Force in 1947. Today, there are more than 40 FFRDCs. Some notable centers include the Jet Propulsion Laboratory, the Los Alamos National Laboratory and Sandia National Laboratories. FFRDCs are governed by the Federal Acquisition Regulation at 48 CFR 35.017.

The purpose of an FFRDC, like its World War II-era forbearers, is to coordinate research between teams of technical experts and to promote technology transfers between the U.S. government and the private sector. Under the FAR, "FFRDC's are operated, managed and/or administered by either a university or consortium of universities, other not-for-profit or nonprofit organization, or an industrial firm." *See* 48 CFR 35.017.

According to the NIST's April 22 Federal Register notice, the contractor selected for the NCCoE's FFRDC will have three primary responsibilities:

- Research, development, engineering and technical support
- Program/project management including, but not limited to, expert advice and guidance in the areas of program and project management focused on increasing the effectiveness and efficiency of cybersecurity applications, prototyping, demonstrations and technical activities
- Facilities management.

The National Institute of Standards and Technology's Computer Security Division has been a leading voice in the cybersecurity world for many years.

LEGAL AND PRACTICAL ISSUES IN COMPETING TO MANAGE AN FFRDC

First things first: Get your house in order

If you are interested in competing to run the cyber FFRDC, your organization will need to overcome a few administrative hurdles in order to be eligible for selection to operate the center.

First, before the NIST goes to market for providers, your organization must satisfy certain basic government contracting prerequisites. For instance, federal contractors must register with the System for Award Management (the SAM was formerly the Central Contractor Registration, or CCR, and the Online Representations and Certifications Application, commonly called ORCA).

To register with the SAM, a contractor will need a taxpayer identification number and a Dun & Bradstreet number, also called a D-U-N-S number, and, once registered with the SAM, a contractor will be issued a commercial and government entity, or CAGE, code. (More information about these processes is contained in the SAM user guide, *available at* https://www.sam.gov/sam/SAM_Guide/SAM_User_Guide.htm).

Second, your organization should implement general compliance policies and procedures, including a written code of business ethics and conduct, and it should have in place a suitable compliance program.[2] These policies and procedures should also address any applicable socioeconomic (*e.g.*, an affirmative action plan) and domestic preference requirements.

Finally, given the sensitive nature of cybersecurity, your organization should anticipate the need to obtain facility and staff security clearances before bidding to work on projects that involve classified information. Although contractors typically will not be issued clearances before the award of a contract, you should consider some of the basic criteria for receiving clearances. These criteria include information about foreign ownership and control, the background of key employees (including their citizenship and criminal history, if any) and whether any employees previously held a

clearance or are undergoing an active background check. Companies must use the Defense Security Service Electronic Facility Clearance, or e-FCL, system to submit an application once a definite, classified procurement need has been established.

Take proactive steps to address potential conflicts of interest

The regulations governing FFRDCs impose restrictions designed to ensure that a managing entity has no conflicts with regard to its position. This is because an FFRDC has access to sensitive and proprietary data, employees and property "beyond that which is common to the normal contractual relationship." FAR Section 35.017(a)(2).

As a result, an FFRDC must "operate in the public interest with objectivity and independence." *Id*. Further, the FFRDC "must be free from organizational conflicts of interest, and ... have full disclosure of its affairs to the sponsoring agency." *Id*.

To emphasize that point, the FAR clarifies that along with universities or nonprofits, the organizations that may operate, manage or administer an FFRDC include industrial firms "as an autonomous organization or as an identifiable separate operating unit of a parent organization." FAR Section 35.017(a)(3).

One means of protecting against conflicts of interest is an agency sponsoring agreement, which is a mandatory feature of all FFRDCs. The sponsoring agreement helps facilitate a long-term relationship between the government and the FFRDC. At a minimum, such an agreement prohibits the FFRDC from competing with any non-FFRDC concern in response to a federal agency request for proposal, or RFP, for anything other than operation of an FFRDC. FAR Section 35.017-1. The FAR clarifies that this prohibition does not apply to any parent organization or other subsidiary of the parent organization in its non-FFRDC operations. On the basis of these requirements, if an organization wants to compete for an FFRDC, it must determine whether its corporate structure can accommodate this type of restriction on its non-FFRDC operations. Some pre-positioning may be necessary to ensure that the parent organization and fellow subsidiaries can operate independent of the FFRDC's activities.

Evaluate agency-specific prohibitions

Sponsoring agreement restrictions not-withstanding, interested parties must also evaluate how the NIST will structure other contractual provisions to guard against conflicts of interest in management of the NCCoE's FFRDC. With increasing frequency, agencies have developed their own definitions of what constitutes an organizational conflict of interest or what business relationships amount to an affiliation that might trigger even the appearance of a conflict of interest. Any such nuances in the NIST's RFP may affect the strategy of a prospective offeror and may necessitate significant efforts to ensure that the organization is pre-positioned to compete for the FFRDC contract.

Monitor and respond to the NIST's FFRDC-related activity

In the next few months, the NIST will publish additional information on the FFRDC. Under the FAR, the NIST is required to publish three notices in the Federal Register indicating the scope and nature of the effort to be performed and to request public comments. The first notification was published April 22, with written comments due by July 22. Any interested party or potential competitor who submits feedback may help the NIST consider aspects of the scope and nature of the effort that it had not

The purpose of a federally funded research and development center is to coordinate research between teams of technical experts and to promote technology transfers between the U.S. government and the private sector.

considered before (especially since some groups have expressed opposition to the proposed FFRDC).

Further, in its initial Federal Register notice, the NIST stated that it anticipated that an RFP would be posted on FedBizOpps.gov,[3] the commonly used government point of entry for federal contracting opportunities. The RFP will lay out what specific requirements offerors must satisfy to be eligible for award of the FFRDC contract. As indicated above, the RFP may also define with more particularity what the NIST believes to be unallowable conflicts of interest that could affect a contractor's ability to effectively manage the FFRDC or that could affect the ability of the organization and its parent or affiliates to compete for similar, non-FFRDC–related work in the future.

Prospective offerors are usually allowed to submit questions to the sponsoring agency to seek clarification on certain terms in the RFP. The identity of each prospective offeror is redacted so as to not reveal competitive decision-making of that organization. Thus, an interested offeror's best chance to affect the language of a procurement is during the Q&A process. Interested parties would do well to monitor FedBizOpps.gov for any requests for information or draft RFPs so they can be ready to pursue the opportunity when it arises.

CONCLUSION

The NIST's proposed cyber FFRDC presents a unique and relatively rare opportunity for a private entity to participate in the development of U.S. cybersecurity policy and forms of technology. The proposal has already triggered significant positive (and negative) attention. Given the unique nature of this opportunity and its increasing public profile, interested parties will want to take the right steps in advance as these steps are critical to competing successfully for the FFRDC solicitation.

NOTES

1 http://www.venable.com/executive-order-opens-consultative-processes-to-draft-cybersecurity-framework-for-critical-infrastructure-02-15-2013/.
2 If industrial firms qualify as "small," they will not be required to possess a compliance program.
3 https://www.fbo.gov/.



Dismas N. Locaria (L), a partner in the government contracts group at **Venable** in Washington, assists government contractors in all aspects of working with the federal government. He can be reached at dlocaria@venable.com. **Andrew Bigart** (C), an associate in the firm's regulatory practice group, can be reached at aebigart@venable.com. **Keir Bancroft** (R), an associate in the firm's government contracts group, can be reached at kxbancroft@venable.com.