Background: Fire protection systems are increasingly networked to Building Control Systems (BCS), Internet of Things (IoT), and other platforms that are, by design or oversight, exposed to the public-facing Internet. This emerging environment could lead to unique and novel cyber vulnerabilities, and attacks on fire protection systems have the potential to have significant consequences. However, a thorough understanding of cybersecurity issues related to fire protection systems is lacking. The expansiveness of these vulnerabilities, the severity of the consequences, and the awareness of the fire protection community of these vulnerabilities is not well understood.

Research Goal: The goal of this project is to assess the cybersecurity threats of built-in fire protection systems connected to BCS, IoT, and other potentially Internet-facing platforms.

Project Tasks: The research goal shall be achieved through the following tasks, which will be conducted under the auspices of the Research Foundation in accordance with Foundation Policies and will be guided by a Project Technical Panel of industry stakeholders:

Task 1: Literature Review.
- Provide an overview of all applicable Codes, Standards, Best Practices, Guides, etc. that deal with subjects with potential cyber vulnerabilities.
- Identify the key stakeholders, their activities, and other attributes.
- Identify common terminology applicable to cybersecurity in fire protection applications.
- Define what fire protection systems or subsystems are vulnerable to cybersecurity threats (e.g. fire alarm systems, electrically monitored fire extinguishers, carbon monoxide detectors, etc.) and identify and categorize potential cybersecurity threats to these fire protection systems.
- Identify and categorize existing prevention and intervention strategies to address identified threats.

Task 2: Case Studies. Conduct a case study review of cybersecurity incidents relevant to fire protection systems. Specifically analyze the vulnerabilities and challenges from each incident and assess the effectiveness of intervention strategies, where available.

Task 3: Workshop and refinement of baseline materials. The baseline materials developed in Tasks 1 and 2 will be further discussed, refined, and evaluated at three phases of the project: (1) Pre-Workshop, (2) During the Workshop, and (3) Post-Workshop.

a) Pre-Workshop Review. All baseline materials developed in Tasks 1 and 2 shall be documented and developed into a draft report and summarized in a PowerPoint presentation to be presented at
the Stakeholder Workshop. These baseline materials shall be reviewed by the Project Technical Panel (PTP) via conference call in preparation for the Stakeholder Workshop. Any feedback received from the PTP shall be modified or further refined prior to the stakeholder workshop.

b) **Workshop Implementation.** FPRF will plan and host a face-to-face workshop which will seek to clarify, confirm, add or refine detailed information and deep insight based on the field experience associated with cybersecurity issues within fire protection systems. The baseline materials developed in Tasks 1 and 2 will be further evaluated, discussed, and refined during the Stakeholder Workshop, in addition to key issues, challenges, or knowledge gaps regarding cybersecurity of fire protection systems.

The logistical details for the workshop including identifying and coordinating attendees, the workshop venue, and overall workshop facilitation will be directly handled by FPRF. The project contractor shall present the findings from Task 2 at the Stakeholder Workshop and participate in Workshop discussion.

c) **Post-Workshop Refinement.** Based on the workshop outcomes and respective feedback, update and refine the baseline materials developed in Tasks 1 and 2. Proceedings documenting the Stakeholder Workshop will be developed by FPRF and published on the FPRF website.

**Task 4: Gap Analysis.**

- Identify knowledge gaps and assess the appropriateness of the existing provisions and guidance related to cybersecurity for fire protection systems.
- Identify and prioritize future research/information needs for cybersecurity of fire protection systems.
- Develop a roadmap to address the cybersecurity challenges associated with fire protection systems.

**Implementation:** This research project is led by the Fire Protection Research Foundation and will be conducted in accordance with the “Research Foundation Policies for the Conduct of Research Projects”. The project will be guided by a Project Technical Panel who will provide input to the project, recommend contractor selection, review periodic reports of progress and research results, and review the final project report.

**Deliverables:** Deliverables addressed by this RFP and handled by the project contractor are:

1) **Interim Pre-workshop Materials** which documents the baseline materials developed in Tasks 1 and 2.

2) **Workshop materials and presentation** which summarizes the baseline information documented in the interim pre-workshop materials that will be presented to the Workshop Attendees.

3) **Draft final and final report** which addresses and evaluates the landscape of cybersecurity concerns and vulnerabilities affiliated with fire protection systems and a research roadmap to address the identified concerns.

**Intellectual Property:** The Research Foundation will retain rights to all project deliverables developed as part of this project, including the project report which will be published on the Foundation website.
**Schedule and Costs:**
This is a fixed price project in the amount of $40,000. All indirect and travel costs incurred are intended to be included within this fixed price. The Foundation does not have a limit on indirect costs, but the total proposal cannot exceed this fixed price.

The project timeline is approximately 7 months in accordance with the following timeline:

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposals Due</td>
<td>10 Jan 2020</td>
</tr>
<tr>
<td>Selection of Contractor</td>
<td>24 Jan 2020</td>
</tr>
<tr>
<td>Work Plan Review (1st Panel Conference Call)</td>
<td>Feb 2020</td>
</tr>
<tr>
<td>Pre-Workshop Report (2nd Panel Conference Call)</td>
<td>Apr 2020</td>
</tr>
<tr>
<td>Stakeholder Workshop</td>
<td>May 2020</td>
</tr>
<tr>
<td>Draft Deliverable Review (3rd Panel Conference Call)</td>
<td>Jun 2020</td>
</tr>
<tr>
<td>Final Deliverables Due</td>
<td>Jul 2020</td>
</tr>
</tbody>
</table>

**How To Respond:** Letter proposals (not to exceed six pages) shall be submitted electronically to Victoria Hutchison, Research Project Manager of the Foundation, at vhutchison@nfpa.org no later than 5:00 pm Eastern time 10 January 2020. For additional details see the “Research Foundation Policies for the Conduct of Research Projects”, the Foundation Operating Principles, and “Research Project Guidelines for Contractors” on the Foundation website at: https://www.nfpa.org/foundation. Each proposal shall include a description of the following which will be used as the basis for proposal evaluation: scope and approach, problem understanding, technical merit, prior relevant experience and personnel expertise, dissemination and distribution strategy, and a detailed budget. This is a fixed price project in the amount of $40,000, which includes any indirect costs and travel to in-person meetings and presentations.

**Note:** This project will proceed only on the basis of receipt of a proposal deemed acceptable to the Foundation and the project sponsor(s). Information on the Foundation’s policies for the conduct of research can be found on our website.