From: **Davis, Jonathan D. (Ctr)** jonathan.davis@nist.gov
Subject: RE: Webform submission from: Collaborate with Us: Technical Contributions
Date: 25 June 2025 at 05:22
To: adam@spqrtech.ai
Cc: NCCoE-NCEP-Team nccoe-ncep-team@nist.gov

Hi Adam,

Thank you for your interest in the NIST National Cybersecurity Center of Excellence (NCCoE) National Cybersecurity Excellence Partnership (NCEP) program.

The National Cybersecurity Excellence Partnership (NCEP) program is an ongoing collaborative partnership between U.S. companies and the NIST's NCCoE with the potential to advance the state of cybersecurity practice. This program fosters rapid adoption and broad deployment of integrated cybersecurity tools and techniques that enhance consumer confidence in U.S. information systems.

NCEP partners pledge to provide hardware, software, and expertise to support our mutual efforts to advance rapid adoption of secure technologies. In addition to contributing equipment and other products to the NCCoE's test environments, organizations may designate guest researchers to work at the center, in person or remotely.

Eligibility: The NCEP program is open to U.S. organizations. Those who qualify and express an interest in joining the NCEP program are reviewed by NIST to determine if the collaboration is feasible and relevant to the NCCoE mission. Organizations accepted into the NCEP program sign a Memorandum of Understanding, including a certification that the organization is not subject to the control of a foreign company or government, to formalize the collaboration with NIST.

Other ways to get involved with the NCCoE:

- *Project Collaborator*: The NCCoE collaborates with organizations on many of its projects. You can respond to a project's Federal Register Notice (FRN) by submitting a letter of interest (LOI) that identifies the product(s) (hardware, software, technical expertise) you can contribute to support the project. NIST evaluates each LOI on a first-come, first-served basis and determines technical acceptability based on fit to the project's scope and satisfaction of the project's technical requirements. View a list of NCCoE projects actively seeking collaborators on our website. Sign up for alerts from us and watch the Federal Register for future calls for participation. Organizations that are selected to participate are required to sign a Cooperative Research and Development Agreement (CRADA). See an example CRADA.

- Sign up for alerts from us and watch the Federal Register for future calls for participation. Organizations that are selected to participate are required to sign a Cooperative Research and Development Agreement (CRADA). See an example CRADA.

- *Community of Interest:* Additionally, companies can get engaged with our research activities via joining a Community of Interest. It's a two-way communication, and we genuinely would like to hear your feedback on our work. You can learn more about our Communities of Interest here.

- For general updates on NCCoE projects and what we're up to, visit our website and follow us on X (formerly known as Twitter) and LinkedIn.

Please let us know if you have any additional questions and if you would like to continue exploring NCEP membership.

Respectfully,
The National Cybersecurity Center of Excellence

From: NCCoE <nccoe-webmaster@nist.gov>
Sent: Thursday, June 12, 2025 6:01 PM
To: NCCoE-NCEP-Team <nccoe-ncep-team@nist.gov>
Subject: Webform submission from: Collaborate with Us: Technical Contributions

Submitted on Thu, 06/12/2025 - 18:00

Submitted by: Anonymous

Submitted values are:

Organization Name
SPQR Technologies Inc

Organization URL
https://spqrtech.ai/

Organization Mission
SPQR Technologies builds cryptographically enforced governance systems for autonomous and AI-driven technologies. Our mission is to ensure that intelligent systems operate lawfully, ethically, and verifiably—under zero-trust conditions and without requiring human oversight. We believe institutional trust should be replaced by cryptographic proof.

Mission Alignment
Our mission directly supports NCCoE's goal of accelerating secure technology adoption. SPQR's architecture leverages post-quantum cryptography, zk-STARKs, and immutable audit chains to deliver verifiable, tamper-proof governance for AI systems. The framework aligns with NIST's zero trust, cybersecurity, and evidentiary integrity principles—offering new enforcement mechanisms for secure, autonomous decision-making.

To support this, we've assembled a secure archive with technical white papers, cryptographic artifacts, and live demonstration videos illustrating the system in action:

🔗 https://bit.ly/3Hg0e4q

We welcome the opportunity to contribute this operational architecture to pilot projects, research initiatives, or CRADA collaborations.

Prior Collaboration with the NCCoE?
No

First Name
Adam

Last Name
Mazzocchetti

E-mail
adam@spqrtech.ai

From: **Adam Mazzocchetti** adam@spqrtech.ai
Subject: Re: Webform submission from: Collaborate with Us: Technical Contributions
Date: 28 July 2025 at 17:42
To: Jonathan D. Davis jonathan.davis@nist.gov
Cc: NCCoE-NCEP-Team nccoe-ncep-team@nist.gov

Hey Jonathan,

Thanks so much for the reply and for laying out how things work with the NCEP program. Honestly, I wasn't sure if I'd already started the ball rolling or if I'd missed a step somewhere, so I really appreciate you clarifying.

Just so you know, I'm genuinely excited about this opportunity. What we've built at SPQR was always meant to be more than just "another security product", it's about putting real, verifiable trust back into systems that are getting more and more complex (and risky) by the day. We'd love to see how our approach can support NCCoE's mission and add some value to what you're doing.

If there's paperwork, more info, or next steps I need to handle, just point me in the right direction, I'm in. Happy to jump on a call too, if that helps speed things up or answer any questions.

Thanks again for the guidance (and patience). Looking forward to taking this further together.

All the best,
Adam

Adam Massimo Mazzocchetti
Founder & Chief Architect
SPQR Technologies Inc.
adam@spqrtech.ai
+61 458 094 464
https://spqrtech.ai

> On 25 Jun 2025, at 05:22, Davis, Jonathan D. (Ctr) <jonathan.davis@nist.gov> wrote:
>
> Hi Adam,
>
> Thank you for your interest in the NIST National Cybersecurity Center of Excellence (NCCoE) National Cybersecurity Excellence Partnership (NCEP) program.
>
> The National Cybersecurity Excellence Partnership (NCEP) program is an ongoing collaborative partnership between U.S. companies and the NIST's NCCoE with the potential to advance the state of cybersecurity practice. This program fosters rapid adoption and broad deployment of integrated cybersecurity tools and techniques that enhance consumer confidence in U.S. information systems.
>
> NCEP partners pledge to provide hardware, software, and expertise to support our mutual efforts to advance rapid adoption of secure technologies. In addition to contributing equipment and other products to the NCCoE's test environments, organizations may designate guest researchers to work at the center, in person or remotely.
>
> Eligibility: The NCEP program is open to U.S. organizations. Those who qualify and express an interest in joining the NCEP program are reviewed by NIST to determine if the collaboration is feasible and relevant to the NCCoE mission. Organizations accepted into the NCEP program sign a Memorandum of Understanding, including a certification that the organization is not subject to the control of a foreign company or government, to formalize the collaboration with NIST.
>
> **Other ways to get involved with the NCCoE:**
>
> - *Project Collaborator*: The NCCoE collaborates with organizations on many of its projects. You can respond to a project's Federal Register Notice (FRN) by submitting a letter of interest (LOI) that identifies the product(s) (hardware, software, technical expertise) you can contribute to support the project. NIST evaluates each LOI on a first-come, first-served basis and determines technical

acceptability based on fit to the project's scope and satisfaction of the project's technical requirements. View a list of NCCoE projects actively seeking collaborators on our website. Sign up for alerts from us and watch the Federal Register for future calls for participation. Organizations that are selected to participate are required to sign a Cooperative Research and Development Agreement (CRADA). See an example CRADA.

- Sign up for alerts from us and watch the Federal Register for future calls for participation. Organizations that are selected to participate are required to sign a Cooperative Research and Development Agreement (CRADA). See an example CRADA.

- *Community of Interest:* Additionally, companies can get engaged with our research activities via joining a Community of Interest. It's a two-way communication, and we genuinely would like to hear your feedback on our work. You can learn more about our Communities of Interest here.

- For general updates on NCCoE projects and what we're up to, visit our website and follow us on X (formerly known as Twitter) and LinkedIn.

Please let us know if you have any additional questions and if you would like to continue exploring NCEP membership.

Respectfully,
The National Cybersecurity Center of Excellence

From: NCCoE <nccoe-webmaster@nist.gov>
Sent: Thursday, June 12, 2025 6:01 PM
To: NCCoE-NCEP-Team <nccoe-ncep-team@nist.gov>
Subject: Webform submission from: Collaborate with Us: Technical Contributions

Submitted on Thu, 06/12/2025 - 18:00

Submitted by: Anonymous

Submitted values are:

Organization Name
SPQR Technologies Inc

Organization URL
https://spqrtech.ai/

Organization Mission
SPQR Technologies builds cryptographically enforced governance systems for autonomous and AI-driven technologies. Our mission is to ensure that intelligent systems operate lawfully, ethically, and verifiably—under zero-trust conditions and without requiring human oversight. We believe institutional trust should be replaced by cryptographic proof.

Mission Alignment
Our mission directly supports NCCoE's goal of accelerating secure technology adoption. SPQR's architecture leverages post-quantum cryptography, zk-

STARKs, and immutable audit chains to deliver verifiable, tamper-proof governance for AI systems. The framework aligns with NIST's zero trust, cybersecurity, and evidentiary integrity principles—offering new enforcement mechanisms for secure, autonomous decision-making.

To support this, we've assembled a secure archive with technical white papers, cryptographic artifacts, and live demonstration videos illustrating the system in action:

🔗 https://bit.ly/3Hg0e4q

We welcome the opportunity to contribute this operational architecture to pilot projects, research initiatives, or CRADA collaborations.

Prior Collaboration with the NCCoE?
No

First Name
Adam

Last Name
Mazzocchetti

E-mail
adam@spqrtech.ai