From: **Davis, Jonathan D. (Ctr)** jonathan.davis@nist.gov
Subject: RE: Webform submission from: Contact Us
Date: 13 June 2025 at 06:49
To: adam@spqrtech.ai
Cc: NCCoE nccoe@nist.gov

JD

Hello Adam,

Thank you for reaching out to the NIST National Cybersecurity Center of Excellence (NCCoE). For solicitation inquiries, we encourage you to visit the NIST Office of Acquisition and Agreements Management site to learn more about how you can do business with NIST.

Here are non-commercial collaborative ways to get engaged with NCCoE:

- *Communities of Interest*: Organizations can get engaged with our research activities by joining a Community of Interest. It's collaborative and we would like to hear your feedback on our work and the cybersecurity challenges facing your organization.
- *Project Collaborators*: 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.
- *Center Partners*: The National Cybersecurity Excellence Partnership (NCEP partnership) is our highest level collaborative partnership between U.S. companies and the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) for the National Cybersecurity Center of Excellence (NCCoE) . This is a long-term, ongoing collaboration. Organizations that are selected are required to sign a memorandum of understanding. If your organization is interested in our NCEP partnership program, we encourage you to complete the form found at the bottom of our If your organization is interested in our NCEP partnership program, we encourage you to complete the form found at the bottom of our NCEP partnership page.
- For general updates on NCCoE projects and what we're up to, visit our website, sign up for alerts from us, and follow us on X (formerly known as Twitter).

Thanks again for your interest in the NCCoE,
The National Cybersecurity Center of Excellence

From: NCCoE <nccoe-webmaster@nist.gov>
Sent: Monday, June 9, 2025 11:03 PM
To: NCCoE <nccoe@nist.gov>
Subject: Webform submission from: Contact Us

Submitted on Mon, 06/09/2025 - 23:03

Submitted by: Anonymous

Submitted values are:

Submitted values are:

First & Last Name
Adam Mazzocchetti

Organization
SPQR Technolgies Inc

Email
adam@spqrtech.ai

Message
Hi NIST committee,

Have you ever faced the challenge of ensuring that autonomous AI systems not only comply with ethical guidelines but can prove it cryptographically, under real-world adversarial conditions?

I'm Adam Mazzocchetti, founder of SPQR Technologies. Over the past couple years, we've been working on an operational system that answers that challenge: the SPQR Governance Framework.

Why this matters:
This isn't just an academic proposal. It's an implemented, zero-trust architecture that uses post-quantum cryptography, zero-knowledge proofs, and tamper-evident logs to turn ethical AI constraints into verifiable, runtime-enforced governance, no human oversight needed.

What's unique:
• Proof, not promises: The system demonstrates ethical compliance in real time, not just in policy documents.
• Immutable logs: We've built a forensic-grade chain of custody that's legally admissible under global evidentiary standards.
• Quantum-ready: We designed it to withstand post-quantum adversaries from the start.

The outcome?
A system that doesn't just align with ethical best practices, it cryptographically enforces them.

I've set up a secure data room with the full white paper, supporting video demonstrations, technical diagrams, and cryptographic proof artifacts. You can access everything here:

https://bit.ly/3Hg0e4q

Let's talk:
I'd love to discuss how we can bring this system into your certification pilots, national security deployments, or international policy initiatives. My goal isn't to sell, it's to see this become the backbone of verifiable, lawful AI everywhere.

Looking forward to your thoughts.

Best,

Adam Massimo Mazzocchetti
Founder & Chief Imperator
SPQR Technologies Inc.
adam@spqrtech.ai
Ph. +61 458 094 464

From: **Adam Mazzocchetti** adam@spqrtech.ai
Subject: Re: Webform submission from: Contact Us
Date: 13 June 2025 at 08:15
To: Davis, Jonathan D. (Ctr) jonathan.davis@nist.gov

AM

Dear Jonathan,

Thank you again for your earlier reply.

Just a quick note to let you know that I've now submitted our information through the official NCEP portal, including our mission alignment statement and access to the secure archive. This archive contains the full white paper, video demonstrations, cryptographic proof artifacts, and supporting architecture for SPQR's evidentiary AI enforcement system.

We're deeply aligned with NCCoE's mission, especially around zero trust, secure governance, and the advancement of auditable AI infrastructure.

I look forward to hearing from your team once the submission has been reviewed, and welcome any next steps or opportunities to contribute to ongoing or upcoming initiatives.

Warm regards,
Adam Mazzocchetti
Founder & Chief Imperator
SPQR Technologies Inc.
adam@spqrtech.ai

On Fri, 13 Jun 2025 at 06:49, Davis, Jonathan D. (Ctr) <jonathan.davis@nist.gov> wrote:

> Hello Adam,
>
> Thank you for reaching out to the NIST National Cybersecurity Center of Excellence (NCCoE). For solicitation inquiries, we encourage you to visit the NIST Office of Acquisition and Agreements Management site to learn more about how you can do business with NIST.
>
> Here are non-commercial collaborative ways to get engaged with NCCoE:
>
> - *Communities of Interest*: Organizations can get engaged with our research activities by joining a Community of Interest. It's collaborative and we would like to hear your feedback on our work and the cybersecurity challenges facing your organization.
> - *Project Collaborators*: 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.
> - *Center Partners*: The National Cybersecurity Excellence Partnership (NCEP partnership) is our highest level collaborative partnership between U.S. companies and the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) for the National Cybersecurity Center of Excellence (NCCoE) . This is a long-term, ongoing collaboration. Organizations that are selected are required to sign a memorandum of understanding. If your organization is interested in our NCEP partnership program, we encourage you to complete the form found at the bottom of our If your organization is interested in our NCEP partnership program, we encourage you to complete the form found at the bottom of our NCEP partnership page.
> - For general updates on NCCoE projects and what we're up to, visit our website, sign up for alerts from us, and follow us on X (formerly known as Twitter)

sign up for alerts from us, and follow us on X (formerly known as Twitter).

Thanks again for your interest in the NCCoE,

The National Cybersecurity Center of Excellence

From: NCCoE <nccoe-webmaster@nist.gov>
Sent: Monday, June 9, 2025 11:03 PM
To: NCCoE <nccoe@nist.gov>
Subject: Webform submission from: Contact Us

Submitted on Mon, 06/09/2025 - 23:03

Submitted by: Anonymous

Submitted values are:

First & Last Name
Adam Mazzocchetti

Organization
SPQR Technolgies Inc

Email
adam@spqrtech.ai

Message
Hi NIST committee,

Have you ever faced the challenge of ensuring that autonomous AI systems not only comply with ethical guidelines but can prove it cryptographically, under real-world adversarial conditions?

I'm Adam Mazzocchetti, founder of SPQR Technologies. Over the past couple years, we've been working on an operational system that answers that challenge: the SPQR Governance Framework.

Why this matters:
This isn't just an academic proposal. It's an implemented, zero-trust architecture that uses post-quantum cryptography, zero-knowledge proofs, and tamper-evident logs to turn ethical AI constraints into verifiable, runtime-enforced governance, no human oversight needed.

What's unique:
• Proof, not promises: The system demonstrates ethical compliance in real time, not just in policy documents.
• Immutable logs: We've built a forensic-grade chain of custody that's legally admissible under global evidentiary standards.
• Quantum-ready: We designed it to withstand post-quantum adversaries from the start.

The outcome?
A system that doesn't just align with ethical best practices, it cryptographically enforces them.

I've set up a secure data room with the full white paper, supporting video demonstrations, technical diagrams, and cryptographic proof artifacts. You can access everything here:

https://bit.ly/3Hg0e4q

Let's talk:
I'd love to discuss how we can bring this system into your certification pilots, national security deployments, or international policy initiatives. My goal isn't to sell, it's to see this become the backbone of verifiable, lawful AI everywhere.

Looking forward to your thoughts.

Best,

Adam Massimo Mazzocchetti
Founder & Chief Imperator
SPQR Technologies Inc.
adam@spqrtech.ai
Ph. +61 458 094 464

From: **NCCoE NCEP Team** nccoe-ncep-team@nist.gov
Subject: Confirmation of your request to join NCEP
Date: 13 June 2025 at 08:00
To: adam@spqrtech.ai

Hello,

Thank you for expressing your interest in having SPQR Technologies Inc join the National Cybersecurity Excellence Partnership (NCEP). Our team will review your submission and reach back out to discuss next steps.

In the meantime, we invite you to explore other ways to get involved with the NCCoE:

- **Become 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. 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:** Watch the Federal Register and receive notices about future calls for participation. Organizations that are selected to participate are required to sign a Cooperative Research and Development Agreement (CRADA).
- **Join a Community of Interest:** Additionally, companies can get engaged with our research activities by 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.
- **Follow Us:** For general updates on our projects and initiatives, follow the NCCoE on Linkedin or X (formerly Twitter).

If you have any questions, feel free to contact us at nccoe-ncep-team@nist.gov
Regards,

The NCCoE NCEP Team

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

JD

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