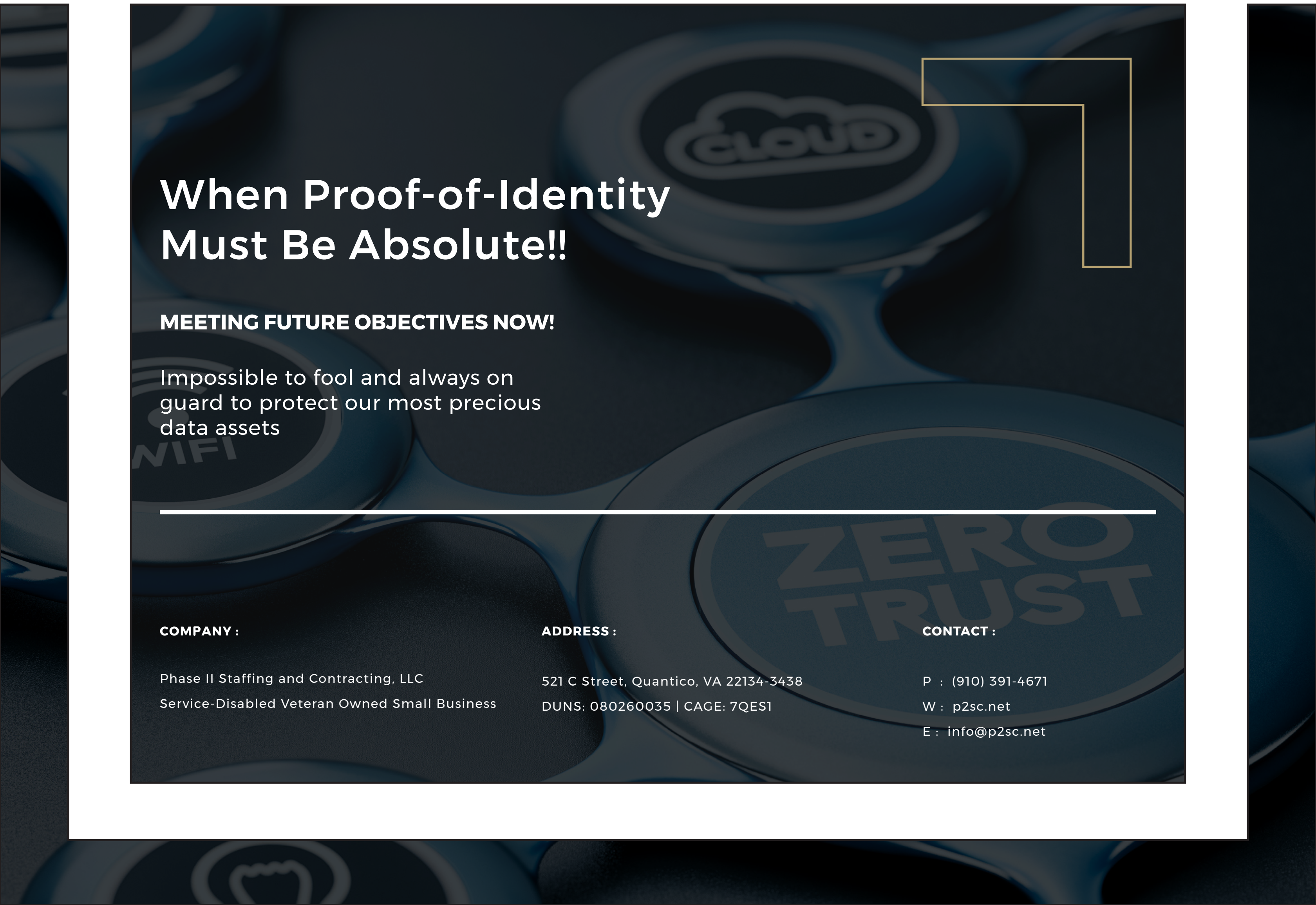
PHASE II

THE OTHER SIDE OF SERVICE

SENTINEL

ZERO TRUST BIOMETRIC ACCESS CONTROL



When Proof-of-Identity Must Be Absolute!!

MEETING FUTURE OBJECTIVES NOW!

Impossible to fool and always on guard to protect our most precious data assets

COMPANY :

Phase II Staffing and Contracting, LLC
Service-Disabled Veteran Owned Small Business

ADDRESS :

521 C Street, Quantico, VA 22134-3438
DUNS: 080260035 | CAGE: 7QES1

CONTACT :

P : (910) 391-4671
W : p2sc.net
E : info@p2sc.net

COUNTERING CURRENT THREATS

COUNTERING CURRENT THREATS

MEETING FUTURE OBJECTIVES NOW!

Current “smart card” and “access badge” technology is not keeping pace with the threat. Like the Soldiers guarding the Tomb of the Unknown, Sentinel, based on the SentryCard, is impossible to fool and always on guard to protect our most precious data assets. Sentinel is the government-facing brand and is designed for organizations seeking an indisputable assurance of:

- Who is entering their facilities and where they are traveling in those facilities allowing for tracing of daily movement
- Who is accessing their computers and devices
- Who is logging into their websites
- The combined biometric and token information granting access

SENTINEL PROVIDES THE FOLLOWING:

- Proof positive biometric authentication for physical and logical access – improved and infallible Multifactor authentication
- **Passive Proximity detection** – eliminates piggybacking, wandering badge holders and much more.
- Automated contact tracing and mustering/accountability
- Biometrics stored within the credential never touching an external database – improved security

ADDED SECURITY, ENHANCED PRIVACY, ENTERPRISE SCALABILITY

Sentinel is the first open-architected biometric platform of its kind

It is self- contained and, once configured to the specific user, disconnected from any network, server, or software, making it undiscoverable.

The biometrics are enrolled, stored and matched solely within the Sentinel, alleviating a broad range of privacy concerns, including General Data Protection Regulation (GDPR) and Biometric Information Privacy Act (BIPA). Sentinel is equipped with Fast Identity Online (FIDO) 2-standards based security keys, providing an unphishable standards-based passwordless authentication method.

The Fast Identity Online (FIDO) Alliance launched in 2013 to develop and promote new authentication standards and end our reliance on passwords. In an online world where many companies now rely on resources working worldwide, cybersecurity remains one of the biggest risks facing every organization today.

FIDO2 is the latest biometric identification security standard published by the alliance, aiming to improve the architecture behind its current protocols. (FIPS 140.2 Certification pending).

WITH FIDO2 IMPLEMENTATIONS, USERS GAIN:

- Added security – Your cryptographic login credentials remain unique across all websites and online services. Personal information stays on the user's device, eliminating the risk of phishing and other forms of password theft.
- Increased convenience – Users have a simple built-in mechanism like a fingerprint scanner to provide fast, secure, and convenient access to online services.
- Enhanced privacy – Cryptographic keys are unique for every website, giving users added privacy as sites cannot track you across the web.
- Enterprise scalability – The implementation of the WebAuthn and FIDO2 specifications use a JavaScript API suitable for most browsers and platforms available today.

To enable near-seamless roll-out, Sentinel integrates with all leading industry platforms and readers, which mitigates or eliminates the need to rip and replace existing infrastructure.

Sentinel was designed to address the Supply Chain Risk Management (SCRM) concerns brought to light by the COVID-19 pandemic and reliance on products made outside of the United States. **Sentinel is produced entirely in the United States of America**. Sentinel addresses the requirements of protecting our Information and Operational Technology, as well as enhancing the Physical Security practices. Sentinel provides multi-factor biometric proof-of-identity for building and system access, including access to areas within facilities.

Zero Trust is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction.

Sentinel's biometric platform provides the missing piece for the only Zero Trust solution currently available. Sentinel is the result of an evolution from keeping honest people more honest to focusing on stopping the dishonest.

Current solutions can be fooled or foiled because they require trust....

- Passwords
- MFA Mobile Authentication
- Text/Mobile solution
- Keypads
- Card Access
- RSA Tokens
- EUSB/A Passwords

Sentinel enables Zero Trust....

- Biometric Authentication (maintained on Sentinel)
- Absolute Proof-of-Identity
- Air Gapped
- Physical Security
- Logical Security
- Operational Security

REQUIRES TRUST	REQUIRES TRUST	TRUE ZERO TRUST
• Passwords • MFA Mobile Authentication • Text/Mobile solution • Keypads	• Card Access • RSA Tokens • USB/A Passwords	• Biometric Authentication • Absolute Proof-of- Identity • Air Gapped • Physical Security • Logical Security • Operational Security
USER AUTHENTICATION	DEVICE AUTHENTICATION	TOTAL AUTHENTICATION

LOGICAL ACCESS, PHYSICAL ACCESS, PROXIMITY DETECTION

Sentinel is the first open-architected biometric platform of its kind

BIOMETRIC LOGICAL ACCESS

Sentinel biometric authentication quickly provides indisputable proof-positive identification for every computer and server login, whether on-site or working remotely. When used in conjunction with FIDO2, or any third-party logical software, Sentinel provides the path to a zero trust architecture. Sentinel enables your organization to move from a “trust-required” to a password less, Zero-Trust future. Sentinel mitigates risks of phishing scams, keyboard logging, and eliminates the cost of your Password Reset Helpdesk!

BIOMETRIC PHYSICAL ACCESS

Sentinel can be integrated into existing physical access control infrastructure, while replacing standalone biometric solutions. Sentinel and its data is undiscoverable until the user is biometrically authenticated, protecting the privacy of the user and the potential liability to the organization.

PASSIVE PROXIMITY DETECTION

With embedded UHF technology, Sentinel can be leveraged to track the location of the credential holder while they are in the office. That’s critical when determining who is inside in the event of a mandatory evacuation. Importantly, in the COVID era, it enables organizations to implement contact tracing and determine how the illness might spread in the unfortunate occurrence of an outbreak. That can be the difference between a site-wide quarantine or targeted quarantining of only the individuals who were exposed. Sentinel provides the ability to identify personnel outside of their authorized areas with colored light or sound.

SENTINEL IS UNIVERSALLY COMPATIBLE WITH EXISTING INFRASTRUCTURE—NO NEED TO RIP AND REPLACE!

	Sentinel Enterprises **Biometric Proximity**	Sentinel Enterprises **Biometric iClass**	Sentinel Enterprises **Biometric SEOS**	Sentinel Enterprises **Biometric EV2/FIDO2**	Sentinel Enterprises **Biometric EV2/FIDO2 non-biometric proximity**
Enroll biometrics on card	●	●	●	●	●
Biometric Data Encrypted AES256 and Security Key	●	●	●	●	●
Enrollment of two different fingers	●	●	●	●	●
FIDO2				●	●
Compatible with Passwordless software & computer login	●	●	●	●	●
Reader Compatibility					
Proximity	●			●	●
iClass		●		●	●
SEOS			●	●	●
EV2				●	●
LEAF EV2				●	●
LEGIC EV2				●	●
Des/Fire/MiFare EV2				●	●

Sample of Compatibility with Access Control Systems. No additional software, API or Integrations Required.

Genetec LENEL:S2 SOFTWARE HOUSE Honeywell openpath brivo

PRIVACY CONCERNS

The protection of biometric data is of paramount importance

Any breach exposing this ultra- sensitive personal data poses significant risks and liabilities to the organization as well as to the affected person.

In order to keep organizations accountable, several U.S. States have passed legislation regarding the collection, storage and use of biometric data. Internationally, the E.U.'s General Data Protection Rights (GDPR) legislation, along with the rules in the UK and India provide a strong stance on biometric data protection and the associated liabilities. The potential liabilities for the mishandling of biometric data are considerable. Illinois' Biometric Information Privacy Act (BIPA) is viewed as the most rigorous, imposing a $1,000 to $5,000 penalty for each violation, per employee, until remedied. In 2018–19, over 200 BIPA lawsuits were filed targeting employers utilizing biometric technology in the workplace.

KEY PRIVACY ATTRIBUTES: Sentinel eliminates most of the risks associated with using biometric authentication by removing all human access to the biometric data.

1 **DECENTRALIZED:** Biometric data is enrolled, stored and matched solely within the Sentinel platform, never touching an external database or server. With Sentinel there is no large "honeypot" of biometric data for hackers to pursue.

2 **UNIQUE:** Each Sentinel generates its own unique inaccessible encryption key used to protect the biometric data stored within the card.

3 **NON-TRANSFERABLE:** Sentinel is a single-use solution. Once a person's biometrics are enrolled only that person can ever use the credential.

4 **CONTROLLED:** Once issued, the holder maintains control of their biometric data, stored securely within the credential.

5 **IRRETRIEVABLE:** Enrollment of the holder's biometrics are one-way and irreversible once set. The credential's only output is an affirmative or negative authentication.

AN IMMEDIATE ROI

WHILE INCREASING SECURITY, MITIGATING RISK AND REDUCING COMPLEXITY.

REDUCTION CATEGORY	AVERAGE COMPANY SPEND	BUSINESS OUTCOME
Eliminate secondary multi-factor authentication, i.e. soft and hard tokens.	$40 per employee annually plus token cost.	Sentinel Payback: **Just over 18 months.**
Significant reduction in Helpdesk Support.	1.2 helpdesk interactions per year at $70 per employee.	Sentinel Payback: **Less than 12 months.**
Eliminate password and phishing training.	$75 per employee annually.	Sentinel Payback: **Immediate** as Sentinel eliminates the need to use usernames and passwords for logical access.
Eliminate the need to upgrade or replace existing readers or add new biometric devices.	$3,000 to upgrade existing readers or $7,500 to install new readers and infrastructure.	Sentinel Payback: **Immediate** as Sentinel credentials automatically turn existing readers into biometric readers.
Eliminate internal IT cost for servers and support for a biometric software solutions.	$50,000–$100,000 annually per server.	Sentinel Payback: **Immediate** as biometrics are enrolled, stored and matched on the Sentinel. No databases, servers or workstations required.
Eliminate the risks associated with the storing employee biometric data.	$10,000 fine per instance for GDPR violations related to the mishandling of biometric data.	Sentinel Payback: **Immediate** as biometrics are enrolled, stored and matched on the Sentinel. No databases, servers or workstations required.

The Sentinel will "plug & play" with your existing infrastructure to provide a secure and touchless solution while addressing today's hygiene and privacy concerns.

GET STARTED TODAY!

SCHEDULE A CONSULT WITH PHASE II TO LEARN MORE ABOUT ALL SENTINEL PRODUCTS!

CONTACT PHASE II

WWW.P2SC.NET

INFO@P2SC.NET

(910) 391-4671

PHASE II

THE OTHER SIDE OF SERVICE

ABOUT PHASE II

Phase II Staffing and Contracting, LLC (dba Phase II) submits this Information Paper for your consideration because securing our critical data cannot wait for a normalized timeline. The threats posed by criminal organizations, State-sponsored cells, and hostile Nations is a threat that must be countered now.

Phase II Staffing and Contracting, LLC

Address:	Phase II 521 C Street, Quantico, VA 22134
Remit to:	Phase II, PO Box 594, Manassas, VA 20108
CAGE Code	7QES1
DUNS No.	080260035
GSA MAS 70 Contract	47QTCA19D003W
Socio Economic Status	Service-Disabled Veteran Owned Small Business
Federal Tax ID No.	81-2416148
Facility Clearance:	TOP SECRET

Phase II, and our partner developers/manufacturers, stands ready to provide a more detailed briefing and a basic demonstration.