

October 30, 2017

Senator Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20510

Dear Senator Wyden:

The men and women of Unisyn Voting Solutions appreciate this opportunity to assure you of our very strong commitment to safeguarding the election process in the United States. Ensuring that every vote is accurately recorded and counted will always be our highest priority.

Our in precinct OpenElect® digital scan voting systems were the first to receive certification from the U.S. Election Assistance Commission under the 2005 Voluntary Voting System Guidelines. Unisyn's voting products are engineered around a streamlined and hardened Linux core, integrating technologies and best practices to deliver multiple layers of security.

Events of the recent past have highlighted the need for comprehensive, formalized and auditable information security practices. To this end we are transitioning our existing processes and procedures into the framework defined in the ISO 27001:2013 standard for information systems security. We look forward to certification by the end of 2017.

Our responses to the queries in your letter dated October 3, 2017, are below:

1. Does your company employ a Chief Information Security Officer? If yes, to whom do they directly report? If not, why not?

The company's IT Director and System Architect cooperate to fulfill the roles and responsibilities equivalent to that of a CISO. Furthermore, every member of Unisyn's technical leadership is charged with maintaining the enterprise vision and strategy of designing and operating technologies that protect the security and integrity of the voting process. These individuals report directly to the president.

2. How many employees work solely on corporate or product information security?

Unisyn's design philosophy is to integrate security at every level of the development process. All technical staff utilize their system security knowledge and experience, supported by the guidelines in the Security Specification document and the VVSG, to build a more secure system.

3. In the last five years, how many times has your company utilized an outside cybersecurity firm to audit the security of your products and conduct penetration tests of your corporate information technology infrastructure?

The company underwent a third-party penetration test in 2017 as part of our ISO 27001:2013 information systems security initiative and we will continue the procedure on a regular basis moving forward. Our voting systems, though not connected to any public or private network, have been subject to penetration testing four times as part of the certification of new software releases.

4. Has your company addressed all of the issues discovered by these cybersecurity experts and implemented all of their recommendations? If not, why not?

Based on the findings of the most recent penetration test, the company has updated its ISMS Risk Register to reflect the findings of the audit, developed controls for addressing them and has implemented mitigation strategies for each. The company has directly and successfully addressed a majority of the findings, and is actively addressing the few remaining items; none of which impact the design, manufacture or development of our products. We will review and update the risks, progress and plan regularly.

5. Do you have a process in place to receive and respond to unsolicited vulnerability reports from cybersecurity researchers and other third parties? How many times in the past five years has your company received such reports?

Because voting systems are designated critical infrastructure, we receive and review DHS updates on a regular basis. An internal committee evaluates each for its relevance to company infrastructure and our voting products.

Our voting systems are inherently and intentionally designed to function disconnected from any external network, both wired and wireless. We believe that this minimizes the avenues that an external party would have to disrupt or influence the voting process. We respond immediately to any discovered vulnerabilities in third party software and operating systems and submit the solutions for federal and state certification.

In recent years we have taken action on advisories that directly impacted our products and IT infrastructure. As an example, we implemented a patch to address the vulnerability identified by CVE-2014-0160, commonly known as the Heartbleed Bug. A decision was made to integrate the Linux patch for the OpenSSL library into the product line even though the systems were not connected to a network.

6. Are you aware of any data breaches or other cybersecurity incidents in which an attacker gained unauthorized access to your internal systems, corporate data or customer data? If your company has suffered one or more data breaches or other cybersecurity incidents, have you reported these incidents to federal, state and local authorities? If not, why not?

No. Furthermore, the company neither collects nor stores any sensitive customer or voter information that can be compromised.

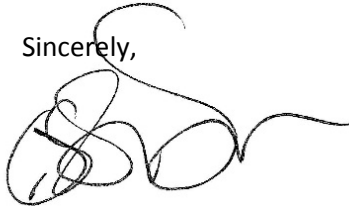
7. Has your company implemented the best practices described in the National Institute of Standards and Technology (NIST) 2015 Voluntary Voting Systems Guidelines 1.1? If not, why not?

We have implemented all of the security components of the VVSG 1.1 as part of our OpenElect 2.0 certification, including a comprehensive review and redesign of our security architecture and enhanced guidance to our customers documented in our best practices guidelines. Implementation of the balance of the VVSG 1.1 guidelines is an ongoing endeavor.

8. Has your firm implemented the best practices described in the NIST Cybersecurity Framework 1.0? If not, why not?

We are implementing the controls outlined in the NIST Cybersecurity framework directly related to components of the ISO 27001:2013 standard. We continually review, refine and expand the ISMS to reflect emerging threats that pose risks to the company's data systems, the information stored therein and our product line.

Sincerely,

A handwritten signature in black ink, appearing to read 'Jeff Johnson', with a long horizontal flourish extending to the right.

Jeff Johnson
President – Unisyn Voting Solutions
760-734-3233