



Hikvision Security Initiative: Network and Information Security Lab

November 25, 2015

To Our Valued Customers,

Hikvision is dedicated to maintaining high standards of cybersecurity for its customers and end-users. This letter serves to provide you with greater insight into this commitment and to introduce you to our Network and Information Security Lab, which upholds the highest level of internal process control, security management, and independent auditing.

Specifically, Hikvision's Network and Information Security Lab is responsible for setting our company's security standards, performing security evaluations and testing, and responding to security issues with third-party security companies. Previously, we introduced the Hikvision Security Response Center (HSRC) Group, an important component of our larger security initiative. Additional Hikvision groups work to minimize the risk of cyberattack on our products:

- The Security Framework Group manages product security framework, sets security standards, maintains SDL procedure, and communicates with third-party companies.
- The Security Component Group develops security components for all product series and researches security protocol.
- The Security Test Group leads offensive and defensive testing and maintains scan tools.
- The Hikvision Security Resource Center (HSRC) Group manages the vulnerability library.

In addition to this in-house cybersecurity team, Hikvision has contracted the renowned US-based security data and analytics company, Rapid7, to perform a penetration test and vulnerability assessment of our products. This includes IP cameras, embedded recorders, and software tools. Rapid7's assessment is underway and is expected to be completed over the next few months.

Another avenue through which Hikvision is ensuring product safety is the Capability Maturity Model Integration (CMMI) certification. On September 18, 2015, Hikvision R&D passed CMMI level 4 certification. A process improvement program, CMMI certification entails control and optimization of development processes, including a standardized development environment, project planning, development tools, and working rules. In keeping with the CMMI standards, Hikvision's software development department has set up mandatory regulations regarding the acquisition of all open source material and downloads of development tools from authorized sources. These tools must be deployed on specified servers for setup, compiling of code, and verification by the dedicated development team. The Network and Information Security Lab audits these processes for compliance.

By setting high standards for product security and following the strict guidelines of reputable outside sources, Hikvision guarantees that its products are of the utmost quality and safety for its customers and end-users. For additional information about Hikvision's commitment to cybersecurity, visit our online security center at http://overseas.hikvision.com/us/about_10636.html

Hikvision USA and Canada