



Colorado Information Analysis Center



**** Alert Bulletin ****

(U//FOUO) Vulnerability of Key Entry Systems within Critical Infrastructure Sectors

(U//FOUO) The Knox-Box[®] rapid entry system is an access control system utilized by public safety agencies. This system allows facilities to securely store entry keys or cards on site for first responders. First responders utilize a master key that unlocks all Knox^{USBUS} boxes within their jurisdiction.¹



(U) Knox[®] Corporation

(U//FOUO) Currently there are over 3.5 million Knox-Box rapid entry systems in use nationwide and over 11,500 fire departments in North America that use the Knox-Box rapid entry system. In one Colorado fire district there are over 4,000 Knox-Box systems in use within the local, state, and federal government which includes; energy, water, postal, emergency services, defense, transportation, and communication sectors.²

(U//FOUO) The Knox-Box system is utilized in numerous ways to include but not limited to:

- Knox Padlocks
- Key switches for gate or other controls
- Electrical shutoffs
- Narcotic storage vaults³



(U//FOUO) Unauthorized access to the system would allow individuals to bypass physical security measures at the site. The unauthorized individuals would also be able to duplicate keys, or remove entry keys or cards which would delay first responders.



(U//FOUO) Master keys for entry systems such as the Knox-Box rapid entry system can be stolen, and older master keys duplicated or fabricated. A single compromised master key will unlock all Knox boxes within the entire jurisdiction.²



(U) Knox[®] Corporation

(U) In February 2014, there were multiple burglaries at several senior assisted living complexes in Minnesota due to illegal access of the Knox-Box system. The master key had been duplicated or compromised and used to open the Knox box.⁴

(U) In January 2014, an audit of a California emergency response organization found that many master keys were unaccounted for, unsecured, or possibly stolen.⁵

(U) In October 2013, an identified USPER was criminally charged with multiple burglaries and possessing a homemade "Master" key used to compromise Knox-Box systems at several apartment complexes in Seattle, WA. There were reports of forty other burglaries associated with the Knox system in 2013.⁶

(U) In February 2013, a researcher with a cybersecurity firm Cylance Inc^{USBUS}, said he created a key capable of opening a Knox box after he obtained a key cylinder for about \$300 and blank keys on eBay for about \$2 each, all of which were mailed to his home. The expiration of keyway patents has allowed the sale of Medeco^{USBUS} key blanks on the internet outside of the manufacturers' control.^{7, 9}

(U) In February 2011, two identified USPERS from Seattle, WA were criminally charged with multiple burglaries after forcibly removing the Knox-Box boxes from businesses, breaking into the boxes, and using the keys inside to enter the business.⁸

(U//FOUO) Recommended protective measures include:

1) Emergency Response Organizations

- a. Utilize effective master key control measures including logging of key serial numbers, who keys are issued to, and maintain secure master key storage
- b. Require key entry systems on critical infrastructure facilities only when necessary
- c. Require the installation and hookup of tamper switches to the buildings burglar alarm system
- d. Consider security factors during installation such as lighting, visibility, video surveillance and ease of access to the Knox-Box
- e. Do not disclose the physical location of Knox boxes, master key storage locations, or method of master key access to the public or those without a need to know
- f. Ensure broken or damaged keys are inventoried, logged, and destroyed in accordance with manufacturer's recommendations
- g. Only install keys from the infrastructure site that are essential for emergency response purposes into the Knox-Box
- h. Ensure keyed lids or lock cylinders are shipped directly to the emergency response organization for final installation and distribution to the end user
- i. Consider upgrading the Knox system to a master key system still under patent protection

2) Critical infrastructure owners and operators

- a. Add additional supplemental security measures to the system such as tamper switches, additional lighting, and video surveillance
- b. Attempt to utilize recess mounted boxes when possible
- c. Ensure lock boxes are securely installed pursuant to the manufacturer's instructions
- d. Install tamper evident seals on keyway covers
- e. Configure access control systems to notify security personnel when emergency response key cards are swiped or access codes are utilized
- f. Add the key box as a location for routine security patrols
- g. Keep a record of keys placed in the Knox-Box including key type and ensure keys are stamped "Do Not Duplicate"

(U//FOUO) Intelligence gaps

- 1) Have there been unreported occurrences of Knox-Box master key thefts or losses in Colorado?
- 2) Have unauthorized individuals accessed critical infrastructure sector sites using these methods?
- 3) Are there other unreported Knox key system vulnerabilities?

(U//FOUO) This report addresses the following CIAC Standing Information Needs: CIAC-SIN-11

Endnotes:

¹ <http://www.knoxbox.com/index.php/knox-rapid-entry-system/fire-departments>

² Colorado Fire Department Terrorism Liaison Officer, personal communication. April 9, 2014

³ <http://www.knoxbox.com/>

⁴ Senior Assisted Living Complexes Seeing a Rash of Break-ins." Senior Assisted Living Complexes Seeing a Rash of Break-ins. Fox Television Stations, Inc, and Worldnow., 8 Mar. 2014. Web. 09 Apr. 2014. <<http://www.myfoxtwincities.com/story/24923116/senior-assisted-living#ixzz2vZ0Wr538>>.

⁵ Jensen, Thom. "Case of the Missing Fire Keys." Case of the Missing Fire Keys. Gannett Company, 21 Jan. 2014. Web. 09 Apr. 2014. <<http://www.news10.net/story/news/2014/01/27/4935045/>>.

⁶ Rosoff, Henry. "Burglary Spree Will Cost Taxpayers \$500,000." Seattle News, Weather, Traffic, Video and Sports. Cox Media Group, 2 Oct. 2013. Web. 09 Apr. 2014. <<http://www.kirotv.com/news/news/half-million-dollar-key-city/nbDmT/>>.

⁷ Finkle, Jim. "Security Expert Warns Fire Department Lockboxes Can Be Hacked." Reuters. Thomson Reuters, 28 Feb. 2013. Web. 09 Apr. 2014. <<http://www.reuters.com/article/2013/03/01/us-security-lockbox-idUSBRE92004T20130301>>.

⁸ Phelps, Matt. "Seattle Men Charged in Bellevue, Redmond and Kirkland Burglaries, Could Also Face Charges in Sony Online Entertainment Server Theft." *Kirkland Reporter*. Kirkland Reporter, 11 May 2011. Web. 09 Apr. 2014. <<http://www.kirklandreporter.com/news/121658229.html>>.

⁹ (U//FOUO) Minnesota Fusion Center – Fire Service Intelligence Analyst, personal communication. March 25, 2014.

CIAC Customer Satisfaction Survey

Please take a moment to complete this survey and help evaluate the quality, value, and relevance of our intelligence product. Your response will help us serve you more effectively and efficiently in the future. Thank you for your cooperation and assistance. [Click here to take survey.](#)

For further information concerning this bulletin please contact the
Colorado Information Analysis Center at (877) 509-2422 or email cdps_ciac@state.co.us
To report suspicious activity, please visit our website at <http://www.dshem.state.co.us>