

RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

March 13, 2024

The Honorable Michael C. Casey
Director
National Counterintelligence and Security Center
LX/ICC-B
Washington, DC 20511

Dear Mr. Casey:

I write to urge the National Counterintelligence and Security Center (NCSC) to warn American businesses about the counterintelligence risks posed by commercial safe locks that do not meet U.S. government security standards.

Many commercially available safes include electronic locks that can also be unlocked using special codes set by and known only to the manufacturer. The existence of these “manufacturer reset” or “management reset” codes is not prominently advertised to consumers, nor the fact that lock manufacturers receive demands from government agencies for those codes. These backdoor codes can be exploited by foreign adversaries to steal sensitive information that U.S. businesses store in safes, such as trade secrets and other intellectual property.

The Department of Defense (DoD), which is responsible for overseeing the standards for locks and safes used to store sensitive and classified U.S. government information, informed my office by email on November 8, 2023, that manufacturer reset codes pose a security threat and, consequently, are prohibited in the locks approved for U.S. government use. DoD also provided my staff with the attached white paper on December 15, 2023, revealing that U.S. government standards for approved locks do not explicitly reference these backdoor codes in order to avoid tipping off the public to their existence. In short, the government has opted to keep the public in the dark about this vulnerability, after quietly protecting government agencies from it.

It would be one thing if these backdoors were only available to U.S. government agencies, but they are not. China-based SECURAM Systems is one of the largest manufacturers of electronic safe locks sold in the U.S. Although DoD has informed my office that the company’s products are not approved for U.S. government use, its low-cost products have enabled the firm to dominate the consumer-focused portion of the market. Technical documents published on the company’s website confirm that its products include manufacturer reset codes, and also indicate that in some cases, consumers may not be told about the existence of these codes. As a China-

911 NE 11TH AVENUE
SUITE 630
PORTLAND, OR 97232
(503) 326-7525

405 EAST 8TH AVE
SUITE 2020
EUGENE, OR 97401
(541) 431-0229

SAC ANNEX BUILDING
105 FIR ST
SUITE 201
LA GRANDE, OR 97850
(541) 962-7691

U.S. COURTHOUSE
310 WEST 6TH ST
ROOM 118
MEDFORD, OR 97501
(541) 858-5122

THE JAMISON BUILDING
131 NW HAWTHORNE AVE
SUITE 107
BEND, OR 97701
(541) 330-9142

707 13TH ST, SE
SUITE 285
SALEM, OR 97301
(503) 589-4555

[HTTPS://WYDEN.SENATE.GOV](https://wyden.senate.gov)

PRINTED ON RECYCLED PAPER

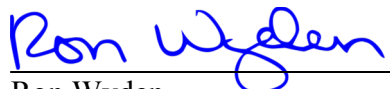
headquartered company, SECURAM is of course obligated to follow Chinese law, including the requirement to cooperate with secret demands for surveillance assistance. Consequently, SECURAM could be forced to share codes with the Chinese government that would enable surreptitious or clandestine access to the safes used by U.S. businesses.

SECURAM's primary U.S.-based competitor, Sargent and Greenleaf (S&G), has confirmed that many of its products include manufacturer reset codes, and that it can be forced to turn over those, both to the government and to civil litigants. The company provided my office with its written policy governing such disclosures, which is also attached. But of course, those codes are also a juicy target for hacking or espionage. Indeed, that is why the only S&G products that are approved to store U.S. government secrets do not feature such backdoor codes.

The NCSC plays an important role in warning U.S. businesses about the espionage threat posed by foreign spies. But U.S. businesses cannot protect their valuable intellectual property, and consequently, America's global economic edge, from foreign espionage if they are kept in the dark about vulnerabilities in the safe locks they use. To that end, I urge the NCSC to update its public educational materials to recommend that businesses upgrade their safe locks to those that meet U.S. government security standards.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,



Ron Wyden
United States Senator

UNCLASSIFIED

Responses to Mr. Chris Soghoian, Senator Wyden

RFI Response, High Security Locks

1. Question: Can you point me to any public document, detailing federal high security lock standards, in which manufacturer reset / management reset codes are prohibited?

Response: The U.S. Government's requirements for a combination lock designed and manufactured specifically to protect unattended national security information is the General Services Administration's FF-L-2740B, Federal Specification regarding Locks, Combination, Electromechanical (available to the public at https://exwc.navfac.navy.mil/Portals/88/Documents/EXWC/DoD_Locks/PDFs/FF-L-2740.pdf). The prohibition on manufacturer reset/management reset codes is contained within the surreptitious entry and covert entry requirements and are not explicitly detailed, since doing so would involve the identification of an entire series of other types of surreptitious and covert entry mechanisms.

2. Question: Is the reason why SECURAM's products are not approved as high security locks for USG use because they feature manufacturer reset/management reset codes, or are there any other national security concerns related to access by foreign governments to data about how their locks work?

Response: OUSD(I&S) does not have knowledge to confirm that SECURAM has submitted any locks for testing, which is a prerequisite for approval. We are unable to speculate on whether any of their locks would be approved or disapproved and on what grounds.

3. Question: With regard to DoD's position that manufacturer reset codes/management reset codes pose a vulnerability, can you please confirm whether this risk is limited to mechanical locks, or does that vulnerability also exist for electronic locks?

Response: Although we cannot provide the formal DoD position via this forum, any master override mechanism would likely be a vulnerability, regardless of the lock type, based on the Federal Specification referenced above.

4. Question: If electrical locks are approved as high security locks, how do the DoD/USG standards address the existence of a mechanism to update the firmware of that lock? For example, can an electrical lock be approved as a high security lock if it features an externally accessible port that can be used to overwrite the lock's firmware?

Response: The FF-L-2740B explicitly prohibits accessible ports.

Sargent & Greenleaf, Inc.

Security Device Access and Legal Process Policy

General Information. Sargent & Greenleaf, Inc. (“S&G”) designs, manufactures, and markets locks and other security devices and mechanisms (“Security Devices”). S&G sells its products to manufacturers that incorporate Security Devices into a wide range of products, including traditional safes for documents and valuables, firearm safes, ATM safes and lock boxes. S&G also sells products through distributors who in turn sell to locksmiths and in some cases individuals (collectively, these manufacturers, distributors, and individuals are “S&G Customers” or “Customers”). Individual consumers are usually customers of S&G Customers (“Consumers”) and may possess a Security Device as a result of purchasing a Customer’s product into which a Security Device has been installed by the S&G Customer.

Security Device Access Information. It is S&G policy that any access to or methods by which to operate any Security Devices installed in Customer products takes place solely at the discretion of S&G Customers and pursuant to any agreements between S&G Customers and any Consumers.

- S&G does not possess any Consumer’s individual access code for any Security Device installed on a Customer product owned or possessed by that same Consumer.
- S&G does not maintain a manifest of which individual Consumers own products fitted with its Security Devices.

Certain Security Devices are designed with manufacturer override/reset codes as a means to assist Consumers and their family members if the security code is lost.

Government and Law Enforcement Requests. S&G policy is to comply with all lawful requests served *directly* on S&G by government agencies and law enforcement pursuant to a lawfully executed and proper warrant, subpoena or court order. S&G will only provide information in response to such lawful requests with a showing of probable cause, or when provided with Consumer or Customer consent, as applicable. S&G carefully reviews all such requests to ensure that there is a valid legal basis for each request, including consulting with legal counsel as appropriate. Once confirmed, S&G complies with legally valid requests. Where S&G determines that there is no valid legal basis or where a request is considered to be unclear, inappropriate or overly broad, S&G will object, challenge or reject the request.

Private Party Requests. For private party requests, S&G complies with the laws pertaining to such requests, subject to the terms and conditions of any Customer contract, any executed subpoena or court order, and applicable law.

Customer Notice. S&G will request that its Customer notify the end use Consumer when access to the S&G Security Device is being sought in response to legal process from government, law enforcement, or third parties, except where providing notice is explicitly prohibited by the legal process itself, by a court order S&G receives, by applicable law or where S&G, in its sole discretion, believes that providing notice creates a risk of injury or death to an identifiable individual, or where notice is not applicable to the underlying facts of the case.

Contact and Requests. Any questions regarding S&G's practices in this area can be directed to S&G at support@sargentandgreenleaf.com. Any requests for information can be formally served on S&G at S&G's corporate office located at One Security Drive, Nicholasville, Kentucky 40356.