



EXECUTIVE VICE PRESIDENT — CHIEF OPERATING OFFICER

OFFICE OF THE PRESIDENT
1111 Franklin Street, 12th Floor
Oakland, California 94607-5200
510/987-0500

October 25, 2017

CYBER RISK RESPONSIBLE EXECUTIVES
CHIEF INFORMATION OFFICERS

President Napolitano recently asked the Cyber-risk Coordination Center (C3) for an analysis, including recommendations, of the risk to the University posed by use of Kaspersky Lab products. As you know, Kaspersky Lab has been linked to the Russian government and cyber espionage, and use of its software has been identified as a potential threat. Both the federal and state governments have developed plans to remove Kaspersky Lab products from their technology environments. See the attached letters from the California Department of Technology and California Cybersecurity Integration Center.

The C3 worked with the location chief information security officers to gather information about the extent to which these products are used at UC and, based on information from publicly available sources, made an overall recommendation for phased removal of these products from the UC environment. The president subsequently approved the recommendation. For more background, please see the attached memo.

Based on the president's approval, effective immediately, UC is placing a systemwide moratorium on the purchase or new deployment of all Kaspersky Lab technologies, including both Kaspersky branded products and other technologies with embedded Kaspersky code.

1. Locations have 45 days from the date of this memo to submit plans for the removal of Kaspersky products and technologies from their environments, either as a stand-alone plan or incorporated into your location's overall cyber plan. The plans should include:
 - a. A six-month plan to stop using Kaspersky-branded technologies. They may request a six-month extension from me if necessary.
 - b. An eighteen-month plan to remove technologies with Kaspersky-embedded code from their environments.

Please submit plans to the Cyber-risk Coordination Center at c3@ucop.edu. If you have questions do not hesitate to reach out to David Rusting at david.rusting@ucop.edu or me at tom.andriola@ucop.edu.

Sincerely,

Tom Andriola
Vice President and Chief Information Officer

Attachments

cc: SVP and Chief Compliance and Audit Officer Bustamante
VP and General Counsel Robinson
AVP and Chief Risk Officer Lloyd
Chief Procurement Officer Cooper
Interim UC Health Chief Procurement Officer Williard
UCACC Chair Borgman
UCACC Vice Chair Martone
Chief Information Security Officers

**DECISION MEMO
(GENERAL)**

To: President Napolitano

From: Tom Andriola, Vice President & Chief Information Officer

Subject: UC's Risk Exposure from Use of Kaspersky Lab Products

Date: October 3, 2017

Summary:

A majority of UC locations use Kaspersky Lab products or components which may pose a cyber-risk. Our ability to fully assess UC's risk is limited because we only have access to unclassified information, however, we believe it is prudent for UC to take steps to mitigate this potential risk.

We now know which UC locations have installed Kaspersky related products and have a better sense of the scale of exposure at each UC location. The actions taken by federal and California state governments with respect to Kaspersky Lab products compel UC to consider similar steps to protect our users, community, and connected IT environments.

We recommend that UC place a systemwide moratorium immediately on the purchase or new deployment of all Kaspersky-branded technologies, and technologies with Kaspersky embedded code. We also recommend that UC locations develop plans with the next 30 days to remove Kaspersky technologies from their environment over the next 6 to 18 months.

Background:

Kaspersky Lab is a Moscow-based firm that primarily provides cybersecurity solutions. In May 2017, senior U.S. intelligence officials testified before the Senate Intelligence Committee that they were reviewing government use of software from Kaspersky Lab.

U.S. intelligence agencies reportedly believe the company and its president have maintained close ties to Russian political and intelligence officials since at least 2012. According to press reports, Kaspersky personnel have accompanied Russian intelligence and police on raids and arrests in Russia, and have designed cybersecurity software to provide the location of possible hackers to Russian law enforcement.

Recent events pertaining to Kaspersky Lab:

- **June 27, 2017:** FBI interviewed Kaspersky employees working for Kaspersky U.S. offices.
- **July 11, 2017:** U.S. General Services Administration removed all Kaspersky products from its list of approved vendors

- **July 18, 2017:** The California Department of General Services and California Department of Technology required all state departments to immediately discontinue use and suspend procurement of any Kaspersky products.
- **September 13, 2017:** Department of Homeland Security instructed all federal executive branch departments and agencies to:
 - Identify any use or presence of Kaspersky products in the next 30 days
 - Develop detailed plans to remove and discontinue present and future use of the products in the next 60 days
 - Begin to implement plan within 90 days of the directive to discontinue use and remove the products from information systems, unless directed otherwise by DHS based on new information
- **September 19, 2017:** Department of Homeland Security clarified that the September 13, 2017, directive applies to Kaspersky-branded products, not to other companies' products that use embedded Kaspersky code.

UC activities related to Kaspersky Lab:

- **July 18, 2017:** All UC locations were asked to provide information about known deployments of Kaspersky products.
- **August 10, 2017:** All UC locations were asked to take a deeper look into their environments, including non-IT and research environments, to identify any Kaspersky products or technologies.
- **August 11, 2017:** A list of known Kaspersky technologies was provided to UC locations. While Kaspersky Lab publishes a list of 67 vendors that use Kaspersky technology in their products, UC's Cyber Coordination Center conducted further research on vendors and identified over 90 vendors.

Discussion/Analysis: The Cyber Coordination Center compiled the following information about Kaspersky Lab technologies installed at UC locations.

Location	Kaspersky Deployed?	Description
ANR	Yes	Kaspersky Anti-Virus (UC Cooperative Extension, Humboldt); 9 Meraki MX Cloud Managed Security Appliances
San Diego Supercomputer Center	Yes	1 Juniper firewall (General environment)
UC Berkeley	Yes	3 computers with anti-virus software (Decentralized departments)
UC Davis	Yes	1 Juniper firewall (Decentralized department); 3 computers with anti-virus software (Decentralized departments)
UC Davis Health	Yes	33 computers with anti-virus software (General environment)
UC Irvine	Yes	1 Watchguard Firebox M400 firewall (Continuing Education Extension)
UCLA	Yes	1 CheckPoint security gateway (General purpose network); Kaspersky Rescue Disk (School of Nursing IT); 1 PineApp Mail Secure Gateway (Anderson School of Management - alumni lifelong email forwarding)
UC Riverside	Yes	4 computers with anti-virus software (College of Natural Agricultural Sciences)
UC Riverside School of Medicine	Yes	Checkpoint Endpoint Protection (UCR School of Medicine IT - 35 servers and close to 300 workstations)
UC San Francisco	Yes	4 Juniper firewalls (General purpose network); 1 Juniper firewall (Children's Hospital, San Ramon); 3 computers with anti-virus software (Otolaryngology Head and Neck Surgery)
UC Office of the President	Yes	1 CheckPoint Security Gateway; 2 computers with anti-virus software

Notes:

- All other UC locations confirmed they do not use Kaspersky Lab products in their environments.
- We do not know whether Kaspersky Lab products are installed on personal devices owned by UC faculty, staff, students, or associates.

Kaspersky Lab provides various cybersecurity products, ranging from desktop computer protection to network traffic protection, and some products pose greater threats than others. We have determined that the biggest potential exposures are firewalls and gateways that utilize Kaspersky technology because a significant volume of network traffic flows through these products.

If Kaspersky Lab products have a “back door,” e.g., a way to control computers or extract data, then those UC locations using firewalls and gateways with Kaspersky technology are at risk. In addition, the UCR School of Medicine may face higher risk due to the scale of its deployment and type of data involved. At other UC locations where there are small numbers of computers running Kaspersky technology, there may be less risk, although these computers potentially could be used to target other systems.

Based on this analysis, the following locations using network-based Kaspersky technology face the greatest exposure:

- ANR
- UCD
- UCI
- UCR
- SDSC
- UCSF
- UCLA
- UCOP

Information from LBNL. Security personnel at Lawrence Berkeley National Laboratory (LBNL) shared with us the approach they are taking, which is based on their knowledge of DOE’s approach and publicly available information. LBNL has made a concerted effort to identify, remove, and block Kaspersky Lab technologies from its environment. LBNL believes that the information available justified removing the products in their open research environment.

Information from Other Research Universities. Other US research universities have been contacted for their analysis and stance on Kaspersky Lab products. The response has been limited to date, but we have found that universities indicated a similar concern about risk and are reviewing the issue. We expect to share our analysis with them.

Options: The options are:

1. Take no action.
2. Continue monitoring the situation and revisit it at later date.
3. Take action to remove Kaspersky technologies from our environment.

While #3 has a cost and temporary IT operational impact across the system, we believe that this is the prudent step to take, given the available information.

Recommendation:

Based on publicly available information, insight from other resources, including LBNL, and the actions of federal and state governments, we believe UC should take action to address the risk posed by use of Kaspersky Lab products.

We recommend a multi-phase approach:

- Place a systemwide moratorium immediately on the purchase or new deployment of all Kaspersky-branded technologies, and technologies with Kaspersky embedded code.
- Have LBNL consult formally with the Cyber Coordination Center to ensure UC has the most current and accurate information available about Kaspersky Lab technologies, including branded technology and technology embedded in other companies' products.
- Direct all UC locations to do the following:
 - By November 1, 2017, develop a 6 month plan to remove using Kaspersky-branded technologies from their environments, with the ability to request a 6 month extension from the UC CIO.
 - By November 1, 2017, develop an 18 month plan to remove technologies with Kaspersky-embedded code from their environments.

Reviewer	Date Routed to Reviewer	Review completion date
1. Cyber Coordination Center (David Rusting)	August 22, 2017	August 24, 2017; comments provided via email
2. Office of General Counsel (Rachel Nosowsky, Mike Troncoso)	August 24, 2017	August 28, 2017; comments provided via email
3. Rachael Nava	August 25, 2017	August 28, 2017; comments & support for document via email (provided)
4.		
5.		
6.		
7.		
REGENT'S OFFICE		

Division Leader Approval – memo preparer will seek Division Leader' final approval before routing to the President's Office.

Date sent to Division Leader:	Approval and date:

President's Decision

Summary Recommendation:

UC should implement a multi-phase approach, as follows:

- Place a systemwide moratorium immediately on the purchase or new deployment of all Kaspersky-branded technologies, and technologies with Kaspersky embedded code.
- Have LBNL consult formally with the Cyber Coordination Center to ensure UC has the most current and accurate information available about Kaspersky Lab technologies, including branded technology and technology embedded in other companies' products.
- Direct all UC locations to do the following:
 - By November ¹⁰~~1~~, 2017, develop a 6 month plan to remove using Kaspersky-branded technologies from their environments, with the ability to request a 6 month extension from the UC CIO.
 - By November ¹⁰~~1~~, 2017, develop an 18 month plan to remove technologies with Kaspersky-embedded code from their environments.

Approve


Disapprove

✓

Modify, as follows: Need to give locations a full

3- days to develop their plans

Needs more discussion with: _____



Janet Napolitano
President

10-10-17
Date



California
DEPARTMENT OF TECHNOLOGY

Joint Communiqué

**Department of General Services
Procurement Division**

707 Third Street, Second Floor,
West Sacramento, CA 95605
(916) 375-4400 (800) 559-5529

**California Department of Technology
Statewide Technology Procurement Division**

10860 Gold Center Drive, Fourth Floor
Rancho Cordova, CA. 95670
(916) 431-5580

Broadcast Date: July 18, 2017

Bulletin #: P-09-17

**TO: Purchasing Authority Contacts (PACs)
Procurement and Contracting Officers (PCOs)
Chief Information Officers (CIOs)
Agency Information Officers (AIOs)**

RE: Kaspersky Anti-Virus Software

On July 12, 2017, the California Cyber Security Integration Center (Cal CSIC) issued a Cybersecurity Advisory stating the United States General Services Administration has removed Kaspersky Lab from two lists of approved vendors used by government agencies to purchase technology equipment.

Consistent with this federal action and in order to protect the integrity and security of the state's information systems and assets, the Department of General Services (DGS), in partnership with the California Department of Technology (CDT), requires all State Departments to immediately discontinue the use of Kaspersky Labs cybersecurity and information technology products and suspend all procurement activities of these products until further notice.

DGS and CDT strongly urge that the Judicial and Legislative branches, along with Constitutional Officers, comply with this bulletin and confirm their current status with CDT.

In addition, Kaspersky Lab products will be removed from all statewide leveraged procurement vehicles until further notice.

For questions regarding this notification, please contact: PAMS@dgs.ca.gov



CYBERSECURITY ADVISORY

12 July 2017

(U) Future selection of Kaspersky Labs products

(U) On 11 July, the United States Government removed Moscow-based Kaspersky ^{USPER} Lab from two lists of approved vendors used by government agencies to purchase technology equipment, amid concerns the cyber security firm's products could be used by the Kremlin to gain entry into U.S. networks.

(U) Last month the Senate Armed Services Committee passed a defense spending policy bill that would ban Kaspersky products from use in the military. The move came a day after the FBI interviewed several of the company's U.S. employees at their private homes as part of a counterintelligence investigation into its operations.

(U) On 12 July, GSA made a tactical decision to remove Kaspersky Labs from two GSA schedules, thus effectively removing the vendor as an authorized source for purchases by any agency using GSA schedules.

- *(U)* The delisting represents the most concrete action taken against Kaspersky following months of mounting suspicion among intelligence officials and lawmakers that the company may be too closely connected to hostile Russian intelligence agencies accused of cyber-attacks on the United States.
- *(U)* Lawmakers raised concerns that Moscow might use the firm's products to attack American computer networks, a particularly sensitive issue given allegations by U.S. intelligence agencies that Russia hacked and leaked emails of Democratic Party political groups to interfere in the 2016 presidential election campaign. Russia denies the allegations.

(U//FOUO) Per the U.S. General Services Administration, "After review and careful consideration, the General Services Administration made the decision to remove Kaspersky Lab-manufactured products from GSA IT Schedule 70 and GSA Schedule-67 – Photographic Equipment and Related Supplies and Services. GSA's priorities are to ensure the integrity and security of U.S. government systems and network and evaluate products and services available on our contracts using supply chain risk management processes".

(U//FOUO) State, Local, Tribal and Territorial government agencies that use GSA contract schedules for ordering IT goods and services and / or Photographic Equipment and Related Supplies and Services, or otherwise have Kaspersky Lab-manufactured products should consider the risk associated with these products and adhere to Federal guidelines.

(U) **Information security professionals should notify the Cal-CSIC immediately at Calcsic.intelligence@caloes.ca.gov for further information.**



TALKING POINTS

13 July 2017

Security Concerns with Kaspersky Labs Products

On 11 July, the United States Government removed Moscow-based Kaspersky Lab from two lists of approved vendors used by government agencies to purchase technology equipment.

The delisting represents the most concrete action taken against Kaspersky following months of mounting suspicion among intelligence officials and lawmakers that the company may be too closely connected to hostile Russian intelligence agencies accused of cyber-attacks on the United States.

- A Senate Armed Services Committee member said in a statement that “ties between Kaspersky Lab and the Kremlin are very alarming.”
- U.S. intelligence agencies believe that the company and its president have had close ties to Russian political and intelligence officials since at least 2012, when a major shakeup of the firm’s executive ranks brought in new members with ties to Russia’s three main intelligence agencies.
- Kaspersky supplies personnel to accompany Russian intelligence and police on raids and arrests, and designed cybersecurity software that provides Russian law enforcement the location of possible hackers, according to press reports.
- The heads of five U.S. intelligence agencies, including the CIA, said they would not be comfortable using Kaspersky products on their networks.

Kaspersky antivirus solutions are integrated in a range of routers, chip and software products from such household names as Cisco, Amazon and Microsoft.

GSA Statement:

“After review and careful consideration, the General Services Administration made the decision to remove Kaspersky Lab-manufactured products from GSA IT Schedule 70 and GSA Schedule 67 – Photographic Equipment and Related Supplies and Services. GSA’s priorities are to ensure the integrity and security of U.S. government systems and network and evaluate products and services available on our contracts using supply chain risk management processes.”