



## Keys to the Cyber Kingdom: Who Are the ICANN Keyholders?

Last Saturday the Internet entered a new epoch. On October 1, the Obama administration (thanks to culpable inaction by the Republican-controlled Congress) handed over the keys to the cyber kingdom to ICANN (the Internet Corporation for Assigned Names and Numbers), an unaccountable, international, “multi-stakeholder” organization.



For *The New American* and the thousands of other independent, alternative media sites, blogs, and organization websites providing information outside the control of the globalist “mainstream” thought cartel, there is obvious concern about how this transition will impact our continued operation. And with so much of the world’s economy and commerce — as well as military, government services, telecommunications, emergency services, medicine, education, and infrastructure — critically tied to, and dependent on, the Internet, concerns about national security, privacy, stability, and censorship under the new ICANN regime are not trifling matters either.

As we [reported recently](#), ICANN has admitted that its cyber security has been breached hundreds of times by outside hackers. However, it’s not only ICANN’s failure to protect against external threats that should be of concern. What about internal threats from those inside ICANN who are entrusted, literally, with the keys to the kingdom? Who are the keyholders, and who are the “master keyholders”? Very little is known about these mysterious individuals and the awesome power they wield.

One of the few public reports about the Internet security keys and keyholders appeared in a 2014 [article](#) by James Ball in the left-wing U.K. newspaper *The Guardian*. Ball was allowed to attend the high-security ceremony of the keyholders in California. “In a nondescript industrial estate in El Segundo, a boxy suburb in south-west Los Angeles just a mile or two from LAX international airport, 20 people wait in a windowless canteen for a ceremony to begin,” Ball wrote. “There is a strange mix of accents — predominantly American, but smatterings of Swedish, Russian, Spanish and Portuguese can be heard around the room, as men and women (but mostly men) chat over pepperoni pizza and 75-cent vending machine soda.”

“It might be a fairly typical office scene, were it not for the extraordinary security procedures that



Written by [William F. Jasper](#) on October 6, 2016

everyone in this room has had to complete just to get here, the sort of measures normally reserved for nuclear launch codes or presidential visits,” *The Guardian* reporter noted. “The reason we are all here sounds like the stuff of science fiction, or the plot of a new Tom Cruise franchise: the ceremony we are about to witness sees the coming together of a group of people, from all over the world, who each hold a key to the internet. Together, their keys create a master key, which in turn controls one of the central security measures at the core of the web.” He describes an elaborate security regimen that sounds like something from a *Mission Impossible* or *Jason Bourne* movie: retinal eye scans, biometric handprints, security cages, lockdown rooms, alarms, keycards, safe combinations. (A video of Ball’s experience at the ICANN ceremony can be viewed [here](#).)

“What these men and women control is the system at the heart of the web: the domain name system, or DNS,” Ball reports. “The master key is part of a new global effort to make the whole domain name system secure and the internet safer: every time the keyholders meet, they are verifying that each entry in these online ‘phone books’ is authentic.”

*The Guardian* report continued:

The east and west coast ceremonies each have seven keyholders, with a further seven people around the world who could access a last-resort measure to reconstruct the system if something calamitous were to happen. Each of the 14 primary keyholders owns a traditional metal key to a safety deposit box, which in turn contains a smartcard, which in turn activates a machine that creates a new master key. The backup keyholders have something a bit different: smartcards that contain a fragment of code needed to build a replacement key-generating machine.

### KGB Keyholders

One of the keyholders is “Russian security expert” Dmitry Burkov, who “has flown in from Moscow for the ceremony.” Burkov goes back to the days of the Brezhnev era of the Soviet Union and worked in the Soviet Academy of Sciences under Soviet dictator (and KGB boss) Yuri Andropov. It was pretty much a certainty back then that scientists who rose through the ranks in the Soviet Academy were not only Communist Party members, but also KGB-controlled assets. Comrade Burkov’s continued rise under Vladimir Putin’s KGB-FSB regime points toward the very strong likelihood that he is an asset of the FSB (the rebranded KGB), which has taken a very strong interest, of course, in cyberespionage and control of the Internet. We have reported, for instance on the outsized and alarming impact that [KGB/FSB asset Yevgeny Kaspersky](#) is having on computer security, with thousands of western banks, corporations, institutions, and government agencies — and millions of consumers worldwide — using Kaspersky software and consulting services.

“The key issue with internet governance is always trust,” Burkov told *The Guardian* reporter. “No matter what the forum, it always comes down to trust.” Indeed, but what has he done to earn the trust that supposedly accompanies selection as an ICANN keyholder? For that matter, how trustworthy are *any* of the 21 keyholders, and how were they selected? If ICANN’s story is to be believed, they simply put out a “wanted” ad on the World Wide Web and asked if anyone was interested in having this cool, awesome responsibility. This is how *The Guardian* describes what occurred: “The initial selection process was surprisingly low-key: there was an advertisement on Icann’s site, which generated just 40 applications for 21 positions.” Hmmm. 7.4 billion people on the planet and only 40 responded to this offer? Sounds like either we’re facing a global glut of motivationally challenged slackers, or ICANN is dishing out an unbelievable narrative. Surely, considering only the millions of professional techies and the tens of millions of computer nerds trolling on the Internet 24/7 in their moms’ basements, at least a



Written by [William F. Jasper](#) on October 6, 2016

few thousand would have responded to ICANN's wild-beyond-imagination invitation. But only 40 applied? And Dmitry Burkov was one of the lucky 21 chosen as a keeper of the keys. That doesn't seem to pass the most basic smell test.

And Burkov is far from the only security concern. You see, according to *The Guardian's* account, it doesn't take all 21, or even 14, or even 7 keyholders to start the security ceremony. Apparently, only a minimum of three keyholders is required to form a masterkey. That means incredibly high stakes are resting on a very few vulnerable, unvetted, and unprotected individuals. Even if they happen to be totally clean and innocent when selected, they are obviously prime targets for bribery, extortion, seduction, cooptation, kidnapping, and murder by governments, corporations, terrorists, and organized crime.

These security issues were among the many serious matters not adequately publicly aired in the Obama administration's mad rush to sever the United States government's stewardship over vital infrastructure and operations of the Internet. Moreover, as we have [pointed out](#), the Obama administration is clearly in violation of Article IV, Section 3 of the U.S. Constitution, which provides that Congress has the exclusive power "to dispose of and make all needful rules and regulations respecting the territory or other property belonging to the United States." This paramount constitutional issue was spelled out, along with other concerns, in a [letter](#) from Senate Judiciary Committee Chairman Charles Grassley (R-Iowa) and House Judiciary Committee Chairman Bob Goodlatte (R-Va.) to Attorney General Loretta Lynch on September 21.

In other words, President Obama had no more authority to transfer the keys to the Internet to ICANN and its undisclosed keyholders than he does to transfer your car keys to your neighbor's teenage son and his unknown buddies. Contrary to the claims of those who describe the Obama-ICANN transfer as an irreversible done deal, the battle for control of the Internet is far from over. Your U.S. senators and representatives and House Speaker Paul Ryan and Senate Majority Leader Mitch McConnell must be put on notice that this fraudulent transfer is unconstitutional and unacceptable. It can be, and must be, reversed when Congress returns from its ill-advised and undeserved recess.

Related articles:

[Obama-UN Internet Surrender: It Ain't Over til Its Over](#)

[Midnight Deadline: State AGs in Court to Stop Obama-UN Internet Transfer](#)

[Obama-UN Internet Takeover Is Just Hours Away](#)

[Assaults on Internet Freedom Threaten All Freedoms \(Video\)](#)

[U.S. Lawmakers Aim to Block Obama's Internet Giveaway](#)

[Internet "Governance" Summit in Brazil Advances UN Control](#)

[The United Nations Grabs for Internet Control \(Video\)](#)

[Chinese Communist to Lead UN Agency Seeking to Control Internet](#)



## Subscribe to the New American

Get exclusive digital access to the most informative,  
non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



**Subscribe**

### What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.