JEB'S CYBER-CORPORATE-WELFARE-AS-SECURITY PROGRAM

Jeb! Bush has issued a cybersecurity policy as an excuse to bitch about Hillary having her own email server when he himself did the same thing (and exposed users when he revealed some but not all of those emails).

Kudos to Jeb! for releasing it — I agree it's a worthy issue to discuss this election (I meant to finish this when the policy was first issued but things got in the way). But Jeb!'s plan is as much a corporate welfare bill (surprise!) as it is a security bill. Indeed, in its introductory language, it explains the policy is designed "to achieve 4% growth and the 19 million jobs that come with it [with] a vibrant and secure Internet." It's about the Internet and the businesses that operate on it first and foremost, and only secondarily about keeping that world secure.

1. Place a Command Focus on Cybersecurity.

In its first section, Jeb! says we need to "place a command focus on cybersecurity." It continues on to present conflicting data about whether cyber-attacks target big companies (which have the resources to protect themselves, he says) or smaller ones. But this comes amid an admission that "poor cyber-security practices" are one of the biggest problems.

2. Restore Accountability within the Federal Government.

Jeb! makes some of his best points when he argues that government needs to be accountable.

> We need presidential leadership to get

> government to take the cybersecurity threat more seriously, fix the vulnerabilities of government systems, and hold government leaders accountable for the security of information entrusted to their care.
>
> [snip]
>
> Leadership means not hiring political hacks or cronies for critical positions that involve cybersecurity. It also means holding executive branch officials accountable for their failure to prioritize cybersecurity and protect the networks under their care.

Jeb! demands we hold executives (presumably including people like FEMA head "heck of a job" Mike Brown) responsible for cybersecurity lapses. I'll come back to this point.

But then Jeb! — whose brother oversaw, and according to some evidence, authorized the exposure of a CIA officer for political gain — jumps from government accountability to Hillary having kept her emails in the same insecure fashion as Bush did (though Hillary didn't release personal information of correspondents when she released them).

> The President also cannot allow cabinet secretaries and senior officials to violate rules and procedures meant to protect classified and national security-related government communications. It should not be too much to ask government officials to abide by the laws and rules in place to safeguard our national security. Secretary Hillary Clinton's growing email scandal highlights reckless behavior by officials entrusted with some of our nation's most sensitive secrets.

3. Increase U.S. Intelligence and Law Enforcement Cybersecurity Capabilities and Strengthen International Cooperation.

After calling for accountability in government, Jeb! calls for reversing reforms put into place after citizens discovered how much domestic spying the spy agencies have been doing and how ineffective some of it was. Curiously, Jeb's! call for restoring funding to defense contractor moneybags NSA doesn't immediately include FBI, which does less outsourcing.

> The National Security Agency and Cyber Command are on the frontlines of defending the United States against cyberthreats. We must stop demonizing these quiet intelligence professionals and start giving them the tools they need. The Federal Bureau of Investigation also needs more resources to fight back against the onslaught of cybercrime.

That's all the more interesting given that this passage immediately precedes contracting reform.

> The Defense committees of Congress are already working on acquisition reform—the President should work with these committees and others to ensure that a byzantine acquisition process is streamlined for cybersecurity defense technologies.

To be fair, the acquisition process *does* need to be fixed. So, too, does the international cooperation Jeb! calls for (though some of this would be impossible if we obviously restored and expanded our dragnet).

4. Create Public-Private Partnerships to Improve Cybersecurity in the Public and Private Sectors.

Just after calling to resume the dragnets that made contractors rich and to make it easier to make those contracts, Jeb! focuses on the need for public and private cooperation. Curiously, in the same policy calling for accountability in government, he insists we can't do the same with the private sector.

> The country needs a President with the experience and trust necessary to mobilize public and private resources to enhance cybersecurity in public and private sectors. And to be clear, this will not be achieved with finger pointing and talking down to industries that have struggled with security while looking the other way as our classified information is handed over to state-sponsored cyberterrorists.

It's against that background that Jeb! calls to reduce barriers to information sharing by giving corporations immunity even while making cybersecurity standards strictly voluntary.

> At a minimum, the government should redouble efforts to: (1) reduce legal and technical barriers to cybersecurity information sharing between the federal government and private sector, and (2) promote best practices for the private sector, including voluntary cybersecurity standards (e.g., through the National Institute of Standards and Technology's ongoing work).
>
> The House of Representatives has passed a bill to facilitate information sharing by, among other measures, providing liability protection to private-sector companies that share cyberthreat

> information with each other or with the government.

Granted, everyone in Congress is about to embrace such an approach with CISA, but it highlights the problem. If we need accountability to fix our security problem, that accountability has to extend to the private sector. And yet corporatists like Jeb! say that would hurt someone's fee fees and prevent us from protecting ourselves.

5. Remove Barriers to Innovation in the Tech Industry.

Maybe Jeb! thought people would stop reading before they got to Section 5 of his "cybersecurity" platform. Because this section has little to do with cybersecurity and instead, everything to do with demanding we fix cybersecurity so tech companies can keep "innovating."

> As part of this national effort to improve cybersecurity, the government must not be an obstacle to innovation in the tech industry. The government's power to incentivize and empower must take precedence over its predilection to regulate and constrain. Because cyberthreats are always evolving, effective cybersecurity requires continuous innovation, which a flourishing tech industry provides.

The thing is, decades of preference for policies that support innovation in tech are one of the things that have made us insecure. That may well have been the right decision, but the choice to let software companies dodge responsibility for their own security with EULAs pawning much of the risk onto users is one thing that got us here.

Indeed, after demanding easier funding for start

ups (which has nothing to do with cybersecurity and probably isn't smart), lower barriers for H1Bs (which may or may not be good policy but has nothing to do with cybersecurity), and lowering business taxes (which has nothing to do with cybersecurity), Jeb! then points out two ways our insecurity prevents us from implementing these nifty innovations safely.

> The Internet and innovation from the tech industry have enormous potential to help address public policy challenges. For example, digital connections between power plants, transformers, substations, and transmission lines allow for better management of the electric grid. With such networks, utilities are better able to anticipate, avoid, or respond to power outages. Using technology we can create a secure online credential for veterans that verifies their military service. Such a credential could allow instant access to medical records online, and help the private sector offer military/veteran discounts online. However, without a secure Internet, these types of initiatives may never reach their full potential.

It is absolutely correct that insecurity makes both of these potentially beneficial innovations risky. But Jeb! hasn't done the math on how to fix that. His policies still conflict between freeing corporations from any accountability for the insecurity of their systems and demanding that those same corporations deliver networks that are secure enough to make these innovations sound.

That is, he want's cost-free (especially to businesses) cybersecurity.

Short of turning the government into a cyber police force guarding private networks (in which case we're going to have to raise business taxes for the businesses outsourcing their own responsibility to the government), this approach

will not work.

It’s great that the OPM hack has clarified how a lack of accountability fosters insecurity. But that’s just as true for Target and Sony. Eliminating any accountability for them while pawning it off on the government is a fool’s game — and a giant new welfare program to boot.