We affirm; resolved: The benefits of domestic surveillance by the NSA outweigh the harms.

Contention One: NSA surveillance benefits security.

Sub-point A: Cyber security.

There's a gross lack of awareness regarding cyber security. **Joseph Menn explains**

As for the upside, so far only a minority of people and businesses are tackling encryption on their own or moving to privacy-protecting Web browsers, but encryption is expected to get easier with more new entrants. Snowden himself said that strong encryption, applied correctly, was still reliable, even though the NSA has cracked or circumvented most of the ordinary, built-in security around Web email and financial transactions. James Denaro, a patent attorney with security training in Washington, was already using Pretty Good Privacy (PGP), a complicated system for encrypting email, before the Snowden leaks. Afterward, he adopted phone and text encryption as well to protect client information. "**One of the results [of the NSA allegations]** we see from Snowden **is an increased awareness across the board about the incredible cyber insecurity**," Denaro said.

In fact, cyber security is being worked on now because of the NSA program. **Menn continues**

Clients are now inquiring how they can protect their data overseas, what kinds of access the states might have and what controls or constraints they could put in with residency or encryption," said Gartner researcher Lawrence Pingree, formerly chief security architect at PeopleSoft, later bought by Oracle. Richard Stiennon, a security industry analyst and author, predicted that security spending will rise sharply. A week ago, Google said it had intensified encryption of internal data flows after learning about NSA practices from Snowden's files, and consultants are urging other big businesses to do the same. Stiennon said that **after more companies encrypt, the NSA and other agencies will spend more to break through, accelerating a lucrative cycle.** "They will start focusing on the encrypted data, because that's where all the good stuff is," Stiennon said.

The impact is improved, effective methods. **The Center for Strategic and International Studies impacts**

When the DSD mitigation strategies or their U.S. equivalent **[NSA mitigation strategies] are combined with "continuous monitoring"** of risk (a term borrowed from the financial risk and audit communities), **they provide corporations and agencies the ability to identify and mitigate the risk of cyber attacks.**

In the last few years, in 2009 and 2010, Australia's Defense Signals Directorate (DSD) and **the U.S. National Security Agency (NSA) surveyed the techniques hackers used to successfully penetrate networks.** NSA (in partnership with private experts) **and** DSD **came up with a list of measures that stop almost all attacks.**

DSD found that **four risk reduction measures block most attacks. Agencies and companies implementing these measures saw risk fall by 85 percent and, in some cases, to zero.** These measures are "whitelisting," which allows only authorized software to run on a computer or network, very rapid patching both operating systems and programs, and minimizing the number of people on a network who have "administrator" privileges. Implementing these four steps eliminates most of the risk of being breached.

Reducing the number of successful cyber attacks is important. **The Ponemon Institute explains in its 2013 study that**

The most costly cybercrimes are caused by denial-of-service, malicious-insider and web-based attacks, together accounting for more than 55 percent of all cybercrime costs per organization on an annual basis.(5)**Information theft continues to represent the highest external costs [for businesses]**, with businessdisruption a close second.(6) **On an annual basis, information loss accounts for 43 percent of total external costs**, down 2 percent from 2012. Business disruption or lost productivity accounts for 36 percent of external costs, an increase of 18 percent from 2012. (1)

Sub-point B: National security.

The Congressional Research Service found

Intelligence officials initially stated that the two **programs have "helped prevent over 50 potential terrorist events"—which appear to encompass both active terror plots targeting the United States homeland and terrorism facilitation activity** not tied directly to terrorist attacks at home or abroad.72 NSA Director General Alexander subsequently clarified these remarks, citing a total of 54 terrorist events. **Forty-two of these involved terrorist plots and 12 involved material support to terrorism.** Of the total number of terrorist events, 53 somehow involved collection pursuant to Section 702. Thirteen of the 54 involved threats inside the United States, and 12 of those cases somehow utilized the phone records held by NSA.73

NSA data storage allows for dots to be easily connected in terrorist plots. **The Washington Post explains**

In nearly hour---long remarks and the interview afterward, Alexander offered his most impassioned defense of a program that is under fire and that he fears could be curtailed or abolished. He said that **the NSA's database**, which former officials say contains billions of phone number records, **is the only way the government can quickly "connect the dots" between suspect foreign numbers and those in the United States.** "Somebody who has a database that can look at the foreign and the domestic numbers can . . . get the information back quickly and can tell you where there's a threat and where there's not," he said.

Sub-point C: International security.

The Electronic Frontier Foundation initializes

As the NSA scoops up phone records and other forms of electronic evidence while investigating national security and terrorism leads, they turn over "tips" to a division of the Drug Enforcement Agency ("DEA") known as the Special Operations Division ("SOD"). FISA surveillance was originally supposed to be used only in certain specific, authorized national security investigations, but information sharing rules implemented after 9/11 allows the NSA to hand over information to traditional domestic law-enforcement agencies, without any connection to terrorism or national security investigations.

Paul Schwartz, professor of law at UC Berkeley, furthers

Finally the 2006 Wiretap Report details the results of wiretaps in terms of arrests as well as the number of motions made and granted to suppress with respect to interceptions. **Wiretaps terminated in 2006 led to the arrest of 4,376 persons and the conviction of 711 persons.** As arrests and convictions often do not occur within the same year as the use of interception devices, these numbers will increase over the next several years. In addition, **law enforcement officials were able to draw on information gathered through wiretaps to impound large amounts of vehicles, weapons, and illegal drugs.** Regarding motions to suppress, the Administrative Office does not provide this information in its 2006 summary report, but it may be calculated from documents that prosecutors file with the Office. In 2006, of the 283 motions to suppress 7 were granted and 61 were reported as pending.

The creation of the Special Operations Division (SOD) helps crack down on drugs. **Reuters continues**

Since its inception, the SOD's mandate has expanded to include narco-terrorism, organized crime and gangs. A DEA spokesman declined to comment on the unit's annual budget. A recent LinkedIn posting on the personal page of a senior SOD official estimated it to be $125 million. Today, **the SOD offers at least three services to** federal, state and local **law enforcement agents: coordinating international investigations** such as the Bout case**; distributing tips from overseas NSA intercepts, informants, foreign law enforcement partners and domestic wiretaps; and circulating tips from a massive database known as DICE.**

This poses a risk to stability. **The UN Office on Drugs and Crime impacts**

Illicit drug funds, laundered or otherwise, **may infiltrate the formal economy and subsequently the political system, endangering** the foundation and the proper functioning of **civil society and leading to social disintegration and anarchy[,]**.158 In some producer/trafficking countries, drug money is reported to have infiltrated the "last crevices of society, politics, the economy, and even cultural and sports activities ... to gain public support and respect, as well as to have an ideal vehicle for money-laundering".159

The magnitude of funds under criminal control poses special threats to governments, **particularly in developing countries, where** the domestic security markets and capital **markets are [unable]** far too small **to absorb** such **funds without quickly becoming dependent on them.**160 **It is difficult to have a functioning democratic system when drug cartels have the means to buy protection, [or] political support** or votes at every level of government and society.161 In systems where a member of the legislature or judiciary, earning only a modest income, can easily gain the equivalent of some 20 months' salary from a trafficker by making one "favourable" decision, the dangers of corruption are obvious.162

Contention Two: The NSA program is flexible.

First, transparency and accountability can be reformed. **The Washington Post explains**
The president plans to name a "high-level group of outside experts" to study the government's surveillance programs and make recommendations on how to make them more effective and accountable. The panel will be asked to make recommendations for ways **to "maintain the trust of the people, [and to] make sure there's no abuse**, and ask how it impacts our foreign policy." He has asked for an interim report in 60 days and a final report by the end of the year.

Second, past mistakes are mended. **Julie Pace furthers**
The National Security Agency declassified three secret court opinions Wednesday showing how in one of its surveillance programs it scooped up as many as 56,000 emails and other communications by Americans not connected to terrorism annually over three years, **revealed the error to the court which ruled its actions unconstitutional and then fixed the problem.** Director of National Intelligence James Clapper authorized the release, part of which Obama administration officials acknowledged Wednesday was prodded by a 2011 lawsuit filed by an Internet civil liberties activist group.

Basically, NSA domestic surveillance is making reforms to solve for the harms the Con will bring up while not compromising the benefits the program has to offer. In this way, the harms are negligible and the benefits are permanent.