November 1, 2009

**To:** National Security Advisor, Intelligence Community

**From:** NSA Director

**Re:** Cyber Capabilities to Address Iran’s Nuclear Program

Iran claims that its centrifuges merely enrich uranium to produce nuclear power. The Iranian program, however, may also be enriching uranium for a nuclear weapons program. The difference between these two enrichment processes will be difficult to discern without in-person inspections. Because Iran has hundreds of centrifuges in operation currently—and permits no inspections—we must assume the worst. Iran is quickly acquiring material for nuclear weapons.

The NSA has anticipated this possibility for some time. In response, we—in conjunction with our counterparts in the Israeli government—have now finished developing a new cyber weapon, a virus. The virus targets and infects the computers that run the Iranian centrifuges. The virus, once operational, passes through four phases. In the first phase, it searches a computer to see if that computer has a programmable logic controller (or PLC, which automates mechanical systems) and runs the Siemans Step 7 software. Intelligence sources tell us the Iranian centrifuges rely on these two things. If the computer does *not* have a PLC and the appropriate software, the virus deletes itself and all traces of itself from the computer. If the computer *does* have a PLC and the appropriate software, the virus proceeds to the next phase. During this second phase, the virus records the centrifuges’ normal operating data over a period of 30-60 days. Once it has these data, the virus moves to a ‘sabotage’ phase. It asks the computer to speed up the centrifuge, until the centrifuge breaks. This disrupts and ruins the uranium enrichment process, forcing the Iranians to replace the centrifuge and to lose uranium (i.e., the uranium in the broken centrifuge cannot be re-used). During this phase, the virus also plays back the recorded data to Iranian engineers on the computer, so that the engineers do not detect a problem with the centrifuge before it has broken. Finally, the virus goes dormant, before cycling back through the second (recording) and third (sabotage) phases again.

The virus travels via networked computers and has no self-destruct mode. Once released, it *could* propagate on computer systems around the world. We designed it to travel clandestinely. Nevertheless, there is some probability that the virus will be detected before reaching its target. Stuxnet is designed to activate when it identifies both a PLC *and* the Siemans Step 7 software Iran uses to process uranium. We therefore expect it will not affect many other computers it encounters, making it difficult for others to detect. Moreover, the Iranian centrifuges are not connected to the internet (i.e., they are air-gapped). An operative needs to deliver the virus on a portable USB drive, and either (i) wait for an engineer to or (ii) personally plug it manually into the local Iranian network responsible for the centrifuges. That presents its own challenges, but also makes widespread dissemination unlikely. Of course, if the virus finds its way onto any internet-enabled computer, it will move quickly around the world. The Iranians might also detect the virus as it cycles between active (i.e., sabotage) and dormant (i.e., recording) phases.

We believe that there is a likely (though not certain) that the virus will (i) destroy a significant proportion of Iranian centrifuges, and therefore (ii) delay the Iranian nuclear program. We do not have a precise estimate of this delay, but our current estimates range from 3 to 36 months.

*Unknowns*

* How long will it take for the virus to infect Iranian systems? This part depends on human intelligence operatives and chance. The longer it takes, the more likely the virus will be ‘discovered’ before reaching its target.
* How long will the vulnerability exist? The virus required significant resources to build (i.e., many people working over many years). Once deployed (and detected), we cannot recycle it for another purpose. Foreign governments will adapt to protect their systems against future attacks. The virus is therefore a single-use asset—and we cannot be certain how long it will be relevant.
* How will other countries view the virus’s deployment? If detected, the United States will be seen as the first country in history to use cyber weapons offensively to attack another country. Other states could view this as an act of war. Precedent does not exist to guide their response, so we do not know what to expect.
* How many other systems will be affected? The virus could inadvertently attack other computers. We cannot guarantee that other civilian and military devices around the world do not have the combination of characteristics found on the computers in the Iranian nuclear program. If they do, these devices would also be vulnerable.