Sudomesh recognizes that, although the NPRM may be motivated by genuine concerns, its implementation would have broad negative consequences, including hindering the charitable efforts of our organization and others like it. While this NPRM may address important aspects of the FCCs duty to protect the spectrum, it does so at the expense of other, equally important aspects of the FCCs mission, such as supporting innovation and providing broadband services.

Sudomesh is engaged in the development of a non-hierarchical mesh network in Oakland, CA. We are currently developing alternative firmware based on OpenWRT for commercially available wireless devices which can be used to deploy mesh networks using an experimental Internet routing protocol called Babel. If put into effect, this NPRM would render unlawful some of our core activities, and the associated public benefits we anticipate.

Sudomesh shares many goals with the FCC itself. We plan to build a community-maintained wireless network in Oakland, California; as our network is built out, it will bring inexpensive Internet to numerous citizens, provide opportunities for many individuals and organizations to develop innovative network-based projects, and support public safety as a redundant network service in case of Internet failure.

The proposed rules, specifically in paragraphs 4(i) and 8(e), require that manufacturers lock their devices so as to prevent unauthorized software from controlling certain radio parameters. Specifically, the software "must not allow the installers or end-users to operate the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved."

Although the NPRM does not specify the reason for the proposed rule-making, it is widely believed that the Commission is acting on behalf of other users of the U-NII bands, and specifically terminal Doppler weather radar (TDWR). Although U-NII devices are required to employ dynamic frequency selection (DFS) to avoid radar operating on these bands, the architecture of modern 802.11 transceivers is such that almost all time-insensitive functions are handled in software, including DFS, and can be disabled if the user has full control of their device.

To better grasp the scope of this issue, consider that the users of a large proportion WiFi-enabled computer running an open source operating system can, in theory, perform this modification. The NPRM goes on to suggest means for preventing such modifications "including, but not limited to the use of a private network that allows only authenticated users to download software, electronic signatures in software or coding in hardware that is decoded by software to verify that new software can be legally loaded into a device[...]."

We acknowledge that the problem the Commission is faced with is real and must be solved. Tampering with DFS can result in dangerous interference with TDWR. With the proposed rules before us, we must ask first whether they solve the problem, and second, whether they will unfairly penalize users.

Regarding the first question, we note that in prominent cases of interference, such as the Utah Broadband case, and the cases detailed in NTIA report 11-473 (San Juan, Puerto Rico) the non-compliant devices were running manufacturer-supplied firmware. It follows that it is not reasonable to believe that the proposed lockdown will completely solve the problem, since in those cases it was not user modification that resulted in non-compliance.

To answer the second question we point out that the most cost-effective way for applicants to implement the proposed rules is a form of digital rights management (DRM) for the device's firmware, which would render unlawful the installation of third party software with low-level access to radio parameters, even if those parameters do not pertain to U-NII band operation or DFS. This means users must rely on the manufacturer's word that the product is secure, and of course radically curtails consumer choice.

Such software control of the radio hardware is being used in creative and beneficial ways, which are only now beginning to be exploited. There are active open source projects which have brought innovations such as polling/time-division multiple access algorithms for channel management, improved link negotiation for long point-to-point links, better security, the ability to deploy highly redundant mesh networks quickly (for example 802.11s), and many more.

Our position regarding the proposed rules is that

1. they would stifle the innovation which has been building around the use of high-bandwidth unlicensed wireless networking, rendering projects such as ours and OpenWRT unlawful,

2. they would unreasonably restrict the choice of software users can install on their device, potentially resulting in security vulnerabilities,

3. there are ways to achieve the desired control of the U-NII bands in hardware, which would be specific to those bands, and that these should be preferred,

4. they would leave innovation in the wireless world to large companies which can afford the development and certification process required by the rule; that would be irresponsible and inefficient.