I reviewed this document as part of the security directorate's ongoing effort to review all IETF documents being processed by the IESG. These comments were written primarily for the benefit of the security area directors. Document editors and WG chairs should treat these comments just like any other last call comments.

This document, “Definitions of Managed Objects for IP Flow Information Export”is a “bis” of RFC 5815, which was published about 2 years ago (April 2010).

This is a longish document (68 pages), and it’s a MIB. Since I am not a MIB expert I focused on the Security Considerations section of the document, which is about a page and a quarter in length. The text in this section is identical to the corresponding section from the version of RFC 5815 that this document is updating.

The security considerations text is clear. It enumerates tables/objects in the MIB that have a MAX-ACCESS other than “non accessible” and that contain data that might be considered sensitive. It notes why these tables/objects might require (read) access security controls. Other text in this section focuses on security issues applicable to MIBs in general. It admonishes users to employ SNMPv3 and to enable crypto security.

I suggest the following minor, editorial revisions:

SNMP versions prior to SNMPv3 did not include adequate security. Even if the network itself is secure (for example by using IPsec), there is no control as to who on the secure network is allowed to access and GET/SET (read/change/create/delete) the objects in these MIB modules.

It is RECOMMENDED that implementers consider the security features provided by the SNMPv3 framework (see [RFC3410] Section 8), including full support for the SNMPv3 cryptographic mechanisms (for authentication and confidentiality).

Further, deployment of SNMP versions prior to SNMPv3 is NOT RECOMMENDED. Instead, it is RECOMMENDED that SNMPv3 be deployed and that cryptographic security be enabled. It is then a customer/operator responsibility to ensure that the SNMP entity granting access to an instance of these MIB modules is properly configured to grant access to objects only to those principals (users) that have legitimate rights to indeed GET or SET (change/create/delete) them.

Stephen Kent 3/6/12 1:04 PM
Deleted: even then,

Stephen Kent 3/6/12 1:04 PM
Deleted: as

Stephen Kent 3/6/12 1:05 PM
Deleted: privacy

Stephen Kent 3/6/12 1:05 PM
Deleted: to

Stephen Kent 3/6/12 1:05 PM
Deleted: deploy

Stephen Kent 3/6/12 1:05 PM
Deleted: to

Stephen Kent 3/6/12 1:05 PM
Deleted: enable

Stephen Kent 3/6/12 1:05 PM
Deleted: giving

Stephen Kent 3/6/12 1:05 PM
Deleted: give

Stephen Kent 3/6/12 1:05 PM
Deleted: the