Mission Operations require a broad set of supporting data to plan and execute a given mission. This data often originates from different sources on disparate networks of varying security classifications (such as NIPR, SIPR, JWICS, NATO and coalition partner enclaves on BICES). As the sensitivity of an operation increases, so does the required degree8.9 ngree3(s o)-5bned an

o3(p)-3(o)-3(rti)3(n)-(n)-3( )]TJETBT1 0 0 1 90 014 656.5 Tm[(n)-3(e)-3(tw)10(o)-3(rks)]TJETBT1 0 0 1 10 014 656.5

Figure 1: HWW Notional System Architecture

In its full three-domain configuration, both the modular HWW server system, as well as a single 1U or 2U HWW tactical system, consist of two directional subsystems with six servers: three servers for the low-to-high subsystem and three servers for high-to-low subsystem. Each directional subsystem hosts a single server in each security domain. The optional peer connection between the directional subsystems in each domain facilitates log file rotation to a specified domain, status notification for data delivery acknowledgement, health status of each node, and virus definition updates.

Mission Operations require the transfer of file-based and streaming support data to the operational network on a regular basis, i.e. weather data, raster data such as maps and imagery, and administrative files such as briefings, documents, and spreadsheets. This sort of data typically originates on networks operating at a lower classification than the operational network. As a result, physical separation and anti-virus protection are of primary importance and the data handling policy enforcement tends to be more basic. If the data originates from a trusted source, the data handling policy enforcement may simply check the file's particular type rather than inspecting the value of specific metadata fields.

Figure 2: Low-to-High File Transfer Example

In the scenario shown in Figure 2, the HWW low-to-high subsystem receives data from a specific host (not shown) via a secure file transfer protocol (SFTP). Once transferred, HWW scans the file for viruses and applies rules prior to transferring the data to a designated storage location on the operational network. All data is virus scanned and ruleset checked once per domain. For example, if data were to pass from the U domain to the S domain then to the TS domain, HWW would check that data three times prior to reaching its final destination. The system configured to send data to HWW on the low side can send data in an automated fashion or via an ad-hoc user request. The orchestration of the transfer to HWW is outside the system boundary for the HWW system so it provides maximum flexibility for the organization. Implementations include automated polling of an