

**INSTRUCTIONS FOR BUILD REVIEW  
BOARD ROLES AND RESPONSIBILITIES  
FOR THE DOT BUILD POLICY  
WPI0042**

**Prepared by:  
WSR-88D Radar Operations Center  
1313 Halley Circle,  
Norman OK 73069**

**APPROVED FOR  
USE AS PRODUCT  
BASELINE &  
SUBMITTED BY:** \_\_\_\_\_

**DATE:** \_\_\_\_\_

**Rex Reed  
Branch Chief, Engineering  
WSR-88D Radar Operations Center**

**DRAFT**  
**Work Practice Instruction for  
Build Review Board Roles and Responsibilities**

**1) BACKGROUND**

Over time the need for minor WSR-88D computer system software updates (releases that can not stand alone) and point builds (releases that can stand alone) has increased for RDA, RPG and OPUP. This increase can be attributed to:

- *The DOC/NOAA and DOD requirement to address Operating System (OS) security vulnerabilities on WSR-88D equipment on a quarterly basis:* The OS patch list depends on results of PatchLink and Nessus security scans conducted every quarter of the calendar year (March 15, June 15, September 15 and December 15). Current DOC/NOAA and DOD policy requires all medium and high risk security vulnerabilities identified by the scans be mitigated or the affected system patched within 30 days of the security scan results being available.
- *Software defects adversely affecting field operations:* Software defects will generally be corrected during the major build cycles unless the defect has critical impacts to operational users. Critical impact defects by definition have substantial adverse effects on field operations and no acceptable work-around exists to overcome the defect.
- *System upgrades or enhancements outside the normal build cycle:* Upgrades and enhancements are necessary at times when the upgrade or enhancement depends on available funding and procurement in the case of services or new equipment. Unlike security patches and correction of software defects, system upgrades and enhancements are typically planned well in advance. However, on occasion, hardware/firmware upgrades are required that are unexpected and therefore not planned in advance.

**2) SCOPE**

This Build Review Board Roles and Responsibilities WPI applies to the establishment of a Build Review Board (BRB) for defining and scheduling update or point software releases. WPI 0040 – **Emergency System Security Patch Process** also applies when the BRB decides to limit the release content to only addressing security vulnerabilities. For major software releases, build content and schedule are proposed by the System Recommendation Enhancement Committee (SREC) and approved by the NEXRAD Program Management Committee (PMC).

This WPI does not address roles and responsibilities associated with the implementation, testing, documentation and fielding of changes approved by the BRB. This information is covered in WPI- 0003 (ENG) **ECP Origination Instructions and Workflow – Under \$100,000** and WPI-0004 (ENG) **ECP Origination Instructions and Workflow \$100,000 to 1,000,000**.

**3) PURPOSE/OBJECTIVE**

The objective is to establish a process that will allow ROC personnel and external stakeholders the opportunity to provide input and be directly involved in the decision making process of formalizing update or point release content and testing and deployment schedules when minor

build releases become necessary.

This WPI addresses the establishment of a Build Review Board (BRB) and the roles and responsibilities of BRB members. The BRB will make the determination when an update or minor build release is required to address security vulnerabilities, field system enhancements or upgrades, or correct software defects.

#### **4) ESTABLISHMENT OF BUILD REVIEW BOARD**

The Build Review Board will be chaired by the Software Engineering Team lead and composed of members from various ROC branches and agency stakeholders. The BRB will convene whenever the need arises. In general, the BRB should convene after security scan results are available and medium and/or high security vulnerabilities have been identified, a critical software defect has been reported to the WSR-88D Hotline by field personnel and immediate action to correct the defect needs to be taken, or a system enhancement or upgrade is planned outside the normal build cycle.

The ECP Project Engineer or WSR-88D IT Security Officer (ITSO) should request, either orally or in writing, the need to convene the BRB to the BRB chair. Upon receiving the request to convene, the BRB chair will notify board members and agency stakeholders of its intent to meet via email at least 3 business days in advance of the scheduled meeting, if possible. The notification will include a list of topics for discussion.

The BRB chair, ECP Project Engineer or WSR-88D ITSO will provide the BRB members and agency stakeholders background information relating to the proposed change(s) at least 1 business day prior to the scheduled meeting whenever possible. At a minimum, the background information should include:

- A detailed description of the problem or justification for change
- Detailed solution to the problem
- Known risks associated with the change
- Testing requirements
- Documentation requirements

The BRB will be responsible for:

- Reviewing and evaluating candidate OS patches or software Configuration Change Requests for possible inclusion in an update or point build release
- Deciding if a point release is warranted
- Establishing the point release number

If a point release is warranted, the BRB will:

- Define point release content
- Define development, testing and deployment schedules
- Make recommendation to ROC management to proceed with the point release

Because of the short time horizon for fielding security patches and to reduce impacts on normal build cycle resources and activities, the integration, testing and deployment schedule for minor releases are substantially compressed relative to the normal build cycle. For each software

change request, the BRB will recommend disposition based on demonstrated operational need, complexity of change, effects on documentation, inherent risk and testing requirements.

The BRB will operate under the following general guidelines when deciding on release content:

- Release content should be limited to reduce overall risk. Content should include only those changes deemed absolutely necessary which either a) eliminate medium or high security vulnerabilities, b) correct software defects which have substantial adverse operational impacts and no acceptable work-around exists (critical impact), c) support system upgrades/enhancements scheduled outside the normal build cycle.
- Documentation requirements and associated publication costs should be considered when deciding on release content.
- Contention of resources including ROC personnel and test bed equipment should be limited to the extent possible to put out the release.
- Release should minimize impacts to normal build cycle schedules.
- Impacts to external systems should be avoided unless the changes are part of a scheduled system upgrade for the external system.

At times, disputes relating to release content may arise. It is intended that all members have an equal voice in the decision making process. If a consensus can not be reached, any disputes concerning whether a release is warranted, the release content, or any other issues of contention which may arise will be adjudicated by the BRB chairperson.

## **5) ROLES AND RESPONSIBILITIES**

The following paragraphs are organized by ROC team, with bullets indicating the roles and responsibilities within each team as they relate to the BRB. The master schedule for an approved build content will be the responsibility of the ECP Project Engineer.

WPI 0040 **Emergency System Security Patch Process** includes additional roles and responsibilities as they relate to security patches.

- a) Configuration Management (CM):**
  - i) Provide impacts and costs of the proposed changes to the BRB as they relate to CM activities.
- b) Software Engineering (SWE):**
  - i) Submit CCRs, if required, that document proposed changes to be included in release.
  - ii) Provide impacts and costs of the proposed changes to the BRB as they relate to SWE activities. This should include costs associated with the design, development, and integration and testing of the proposed changes.
  - iii) Provide risk assessment to the BRB for all proposed changes.
- c) System Documentation Team (SDT):**
  - i) Work with change originator to determine documentation requirements of any proposed changes.
  - ii) Provide impacts and costs of the proposed changes to the BRB as they relate to SDT activities. This should include documentation effort and publication costs.
- d) System Engineering (SE):**
  - i) Provide the security scan results to the BRB

- ii) Provide impacts and costs of the proposed changes to the BRB as they relate to SE activities. The impacts and costs will depend on changes proposed.
- e) **Radar Support Team (RST):**
  - i) Provide impacts and costs of the proposed changes to the BRB as they relate to RST activities. This should include contention of test personnel and testbed equipment, and any delays the update or point release may cause to the normal build cycle activities.
- f) **Hardware Engineering (HE):**
  - i) Provide impacts and costs of the proposed changes to the BRB as they relate to HE activities.